UNISYS

CTOS®

Remote Access Facility (RAF)

Installation, Administration, and Operations Guide

Release R3.2

Priced Item

September 1993
Printed in US America
4393 5931-000

UNISYS

CTOS®

Remote Access Facility (RAF)

Installation, Administration, and Operations Guide

Copyright © 1993 Unisys Corporation
All rights reserved.
Unisys is a registered trademark of Unisys Corporation.
CTOS is a registered trademark of Convergent Technologies, Inc., a wholly owned subsidiary of Unisys Corporation.

Release R3.2

Priced Item

September 1993
Printed in US America
4393 5931-000

The names, places and/or events used in this publication are not intended to correspond to any individual, group, or association existing, living or otherwise. Any similarity or likeness of the names, places, and/or events with the names of any individual, living or otherwise, or that of any group or association is purely coincidental and unintended.

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THE DOCUMENT. Any product and related material disclosed herein are only furnished pursuant and subject to the terms and conditions of a duly executed Program Product License or Agreement to purchase or lease equipment. The only warranties made by Unisys, if any, with respect to the products described in this document are set forth in such License or Agreement. Unisys cannot accept any financial or other responsibility that may be the result of your use of the information in this document or software material, including direct, indirect, special or consequential damages.

You should be very careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used.

The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Comments or suggestions regarding this document should be submitted on a User Communication Form (UCF) with the CLASS specified as "Documentation", the Type specified as "Trouble Report", and the product specified as the title and part number of the manual (for example, 4393 5931-000).

Unisys is a registered trademark of Unisys Corporation.

CTOS and SuperGen are registered trademarks of Convergent Technologies Inc., a wholly owned subsidiary of Unisys Corporation.

CTOS Application Automator, InControl, Device Service, and Context Manager are trademarks of Unisys Corporation.

IBM is a registered trademark of International Business Machines.

SNA is a trademark of International Business Machines Corporation.

BNA, DCA, V-Series ,and A-Series are trademarks of Unisys Corporation.

XVT is a trademark of XVT Software, Inc.

Page Status

Page	Issue
iii	Original
iv	Blank
v through ix	Original
x	Blank
xi through xx	Original
1-1 through 1-9	Original
1-10	Blank
2-1 through 2-8	Original
3-1 through 3-12	Original
4-1 through 4-17	Original
4-18	Blank
5-1 through 5-5	Original
5-6	Blank
6-1 through 6-11	Original
6-12	Blank
7-1 through 7-34	Original
8-1 through 8-12	Original
A-1 through A-3	Original
A-4	Blank
B-1 through B-2	Original
C-1 through C-3	Original
C-4	Blank
D-1 through D-105	Original
D-106	Blank
Glossary-1 through 10	Original
Index-1 through 18	Original

Contents

About This Guide xv

Section 1. Overview

What Is RAF? 1-2
How RAF Works 1-2
RAF Features 1-6
RAF Components 1-8
Event Generation 1-9

Section 2. Installing and Configuring RAF

Before You Begin 2-2
Preparing the Installation Diskettes 2-2
Determining Which Installation Command to Use 2-2
Determining Which RAF Components to Install 2-3
Installing RAF 2-4
Installing RAF on BTOS, CTOS, AND CTOS/XE Systems 2-4
Installing RAF from a Server 2-6
Configuring RAF 2-6

Section 3. Configuring RAF Networks

RAF Networks 3-2
Local and Wide Area Networks 3-7
Unisys Mainframe Connectivity 3-8
IBM SNA Connectivity 3-10
Which RAF Components to Use 3-11
Documenting Your Network Configuration 3-12

Section 4. Customizing the RAF Environment

What Are Source and Target User Profiles? 4-1
Security 4-2
Security Hierarchy 4-3
Creating and Modifying Source User Profiles 4-4
Signing on to the Source User Profile Utility 4-4
Changing the Administrator Name, Password, or Encryption Status 4-5
Creating a Source User Profile 4-6
Modifying or Deleting Source User Profiles 4-7
Enabling and Disabling Security 4-7
Creating a Magnetic Card Reader (MCR) Profile 4-7
Creating Target User Profiles 4-10
Signing on to the Target User Profile Utility 4-10
Changing the Administrator Name, Password, or Encryption Status 4-11
Creating a Target User Profile 4-12
Modifying or Deleting Target User Profiles 4-13
Enabling and Disabling Target Security 4-13
Defining a Log File 4-13
Setting Source Monitoring Privileges 4-14
Encrypting RAF Passwords 4-14
Script Files 4-15
Creating a Script File 4-15
Using the Script File 4-17

Section 5. Configuring a RAF Telephone Directory

Creating a Telephone Directory Entry 5-1
Modifying or Deleting Telephone Directory Entries 5-2
Using the Telephone Directory 5-4
Exiting From the Telephone Directory 5-5

Section 6. Loading and Unloading RAF Services

RAF Loading Sequence 6-2
Mouse Redirection 6-3
RAF Bridge 6-3
Loading RAF Bridge 6-3
Unloading RAF Bridge 6-4

RAF Target 6-5
Loading RAF Target 6-5
Unloading RAF Target 6-8
RAF RS-232 Target Interface Service 6-9
Loading RAF RS-232 Target Interface Service 6-9
Unloading RAF RS-232 Target Interface Service 6-10
Performance Gathering Service (PGS) 6-11
Loading PGS 6-11
Unloading PGS 6-11

Section 7. Managing a Distributed Environment With RAF

Using Online Help 7-1
Establishing Connections with RAF Targets 7-2
Establishing Connections with RAF Source 7-3
Error Detection and Recovery 7-6
Starting RAF Source and RAF RS-232 Source 7-6
Logging On to RAF Source and RAF RS-232 Source . 7-8
Using the Dial-Up Menu 7-9
Selecting a Node 7-10
Selecting a Target 7-11
Selecting a Partition 7-13
Monitoring Workstations 7-14
View Mode 7-15
Action Keys for View Mode 7-16
Control Mode 7-17
Starting a Control Session 7-17
Action Keys for Control Mode 7-18
Remote Debugging 7-19
Starting a Remote Debugging Session 7-19
Scan Mode 7-20
Starting a Scan Mode Session 7-20
Action Keys for Scan Mode 7-21
Displaying CPU Status 7-22
Starting the Interactive Performance Monitor ... 7-23
Keys for the Interactive Performance Monitor ... 7-23
RAF Target Action Keys 7-24
Redirecting Printer Output 7-25
Changing the Video Update Time Interval 7-25

Recording and Playing Back Sessions 7-26
Starting a Recording Session 7-26
Naming the Record File 7-27
Stopping a Recording Session 7-29
Playing Back a Recorded Session 7-30
Transferring Files 7-32
Using Chit-Chat 7-33

Section 8. Sending Messages to Other RAF Users

About Message Posting 8-1
Message Posting Components 8-3
Loading Message Posting 8-4
Creating Messages 8-5
Saving a Message 8-6
Recalling a Saved Message 8-7
Sending Messages 8-8
Sending a Message to Other Users on Your Cluster LAN 8-8
Sending a Message to Users on Other BNet Nodes . . . 8-10
Sending a Message to All Users in Your Network 8-10
Sending a Message to the Members of a Distribution List 8-11
Displaying Received Messages and Acknowledgements . 8-11

Appendix A. Status Codes

Appendix B. RAF Component Worksheet

Appendix C. Connecting RS-232 Channels

RS-232 Channel Specifications C-1
Direct Connect RS-232 Cable Wiring C-3

Appendix D. Event Reporting

Introduction D-1
CTOS RAF Event Summary D-1
RAF Source Event Message Details D-9
RAF Target Event Message Details D-30
RAF Bridge Event Message Details D-54
RAF RS-232 Target Interface Event Details D-60
RAF Source/Target User Profile Utility Event Details D-69
Performance Gathering Service (PGS) Event Details D-80
Message Posting (MP) Bridge Event Details D-87
Message Posting (MP) Service Event Details D-96
Message Posting (MP) Terminal Event Details D-105

Glossary Glossary-1

Index Index-1

Figures

1-1.	Basic RAF Configuration	1-3
1-2.	Basic RAF Network	1-4
1-3.	Basic RAF SuperGen Series Network	1-5
3-1.	BNet II Network Connecting Cluster LANs	3-3
3-2.	Modem Service Network	3-4
3-3.	Supported Networks and Extended BNET Network	3-5
3-4.	Supported Networks and Extended BNet II Network	3-6
3-5.	Modem Service Wide Area Network	3-7
3-6.	Unisys A/V Series Mainframe Connectivity	3-8
3-7.	Unisys 1100/2200 Series Mainframe Connectivity	3-9
3-8.	IBM SNA Connectivity	3-10
4-1.	Security Hierarchy	4-3
4-2.	Source User Profile Log On Screen	4-4
4-3.	Source User MCR Profile Form	4-8
4-4.	Create Target Profile Window	4-12
5-1.	Create Directory Screen	5-2
5-2.	Update Directory Screen	5-3
5-3.	Modify Directory Screen	5-4
6-1.	Duplicate Target ID Resolution	6-8
7-1.	Example of a Help Screen	7-2
7-2.	Establishing Connections with RAF Source	7-4
7-3.	Establishing Connections with RAF RS-232 Source	7-5
7-4.	RAF Source Log On Menu	7-8
7-5.	Dial-Up Menu Screen	7-9
7-6.	RS-232 Node Selection Menu	7-10
7-7.	Target Selection Screen	7-11
7-8.	Interactive Performance Monitor Screen	7-22
7-9.	RAF Recording Sample Configuration	7-28
7-10	Playback Help Bar	7-30
7-11.	Chit-Chat Screen	7-34

8-1. Message Posting on a Cluster LAN 8-2
8-2. Message Posting on a BNet II Network 8-2
8-3. Message Posting Screen 8-6
8-4. Saving a Message 8-7
8-5. Recalling a Message 8-8
8-6. Message Posting User Name Screen 8-9

C-1. Null-Modem Cable Connection C-3

Tables

1-1. Overview Terms 1-1
1-2. RAF Networks and Protocols 1-3
1-3. RAF Features 1-6
1-4. RAF Components 1-8

2-1. Installation and Configuration Terms 2-1
2-2. RAF Services Diskette Selection 2-3
2-3. RAF Configuration File Parameters 2-7

3-1. Networking Terms 3-1
3-2. RAF Networks 3-2
3-3. Which RAF Components to Use 3-11

4-1. Profile Utilities 4-1
4-2. Source User Profile Logon Function Keys 4-5
4-3. MCR Profile Parameters 4-8
4-4. MCR Profile Example With Fixed-Length Password 4-9
4-5. MCR Profile Example With Variable-Length Password 4-9
4-6. Target User Profile Logon Function Keys 4-11
4-7. Script File Window Parameters 4-16

6-1. RAF Loading Sequence 6-2
6-2. RAF Load Bridge Parameters 6-4
6-3. RAF Load Target Parameters 6-6

7-1. Process for Establishing RAF Target Connections 7-3
7-2. RAF Source and RAF RS-232 Source Parameters 7-7
7-3. Node Selection Menu Options 7-10
7-4. Target Selection Function Keys 7-12
7-5. Partition Selection Function Keys 7-13
7-6. Monitoring Modes 7-14
7-7. Action Keys for View Mode - Source 7-16
7-8. Action Keys for Control Mode 7-18
7-9. Action Keys for Remote Debugging 7-20
7-10. Action Keys for Scan Mode 7-21
7-11. Elements of the Interactive Performance Monitor Display 7-23
7-12. Keys for the Interactive Performance Monitor 7-24

7-13. Action Keys for View Mode - Target 7-24
7-14. RAF Start Screen Recording Parameters 7-27
7-15. RAF Recording File Name Examples 7-29
7-16. Playback Keys 7-31

8-1. Message Posting Components 8-3
8-2. Message Posting Loading Sequence 8-4
8-3. Commands for Loading and Unloading 8-4

C-1. Channel Specifications C-2

D-1. RAF Source Event Summary D-2
D-2. RAF Target Event Summary D-3
D-3. RAF Bridge Event Summary D-5
D-4. RAF RS-232 Target Interface Event Summary D-5
D-5. RAF Source/Target User Profile Utility Event Summary D-6
D-6. RAF Performance Gathering Service (PGS) Event Summary ... D-6
D-7. RAF Message Posting Bridge (MP Bridge) Event Summary D-7
D-8. RAF Message Posting Service (MP Service) Event Summary .. D-8
D-9. RAF Message Posting Terminal Event Summary D-8

About This Guide

This guide contains installation, configuration, and operations information for CTOS Remote Access Facility (RAF).

Who Should Use This Guide

This guide is for all RAF users, including:

- Network administrators or customer support engineers installing, configuring, and using features of RAF
- Users who need reference and procedural information to load RAF and use RAF programs, utilities, and services
- Users who need reference and procedural information to monitor or control another workstation

How To Use This Guide

The guide is arranged in a logical progression of concepts and operations to help you understand and use the features of RAF. The following table lists sections of this book that are of use to new or experienced RAF users.

If you are a	read
New RAF user	Section 1 and 2 first Sections 3 through 8 as you need them
Experienced RAF user	Sections 2 through 8 as you need them

How This Guide Is Organized

The following table depicts how this guide is organized.

Section/ Appendix	Section/Appendix Title	Contents
1	Overview	descriptions of RAF components and features
2	Installing and Configuring RAF	procedures to install RAF and set up the *RAFConfig.sys* file
3	Configuring RAF Networks	configuration diagrams and network planning tips
4	Customizing the RAF Environment	procedures to set up RAF security, Source and Target user profiles, and script files
5	Configuring a RAF Telephone Directory	procedures to create and use the Telephone Directory
6	Loading and Unloading RAF Services	procedures to load and unload RAF
7	Managing a Distributed Environment with RAF	procedures to invoke Help, monitor and transfer files, display CPU status, record and play sessions, and establish chit-chat sessions
8	Sending Messages to Other RAF Users	procedures to create, send, and store messages
A	Status Codes	list of status codes
B	RAF Component Worksheet	RAF Component Worksheet
C	Connecting RS-232 Channels	information on configuring a null-modem cable
D	RAF Events	information on RAF Event generation

Use the following table to locate sections of this guide that contain information that helps you in specific activities.

Activity	Where to Find
Installing RAF Setting up the RAF configuration file	Section 2
Understanding the network Selecting RAF components for the network	Section 3
Creating user profiles Setting up security Creating a script file	Section 4
Creating and using Telephone Directory entries for a dial-up connection	Section 5
Loading RAF, Source, and Target Loading RAF Performance Gathering Service (PGS)	Section 6
Logging on to RAF Using the Dial-up menu Selecting a node, Target, or partition Selecting an alternate list of nodes	Section 7

Activity	Where to Find
Monitoring a Target Transferring files Monitoring a Target's CPU usage Recording and playing back a Target session Using Chit-Chat	Section 7
Creating, sending, displaying, storing and recalling messages	Section 8

Conventions

This guide employs various typographical conventions. The following table lists these conventions.

Item	Convention	Example
command names	bold	Use the **RAF Load Target** command to ...
defined terms	italic	A *RAF bridge* is ...
field names	italic	The *User Name* field ...
file names	italic	Type *[Sys]<Sys>TargetProfile.sys* to ...
keycap names	all caps, bold	Press **RETURN**.
key combinations	all caps, bold, keycap names separated by +	Press **ACTION+T** to invoke ...

Diagrams

For ease of understanding, some RAF screens omit certain details, such as indications of RAF release levels or objects not critical to the text. The diagrams depict menu selections and functionality accurately.

ACTION + Quote

You can use ACTION key combinations within RAF programs. The ACTION + ' combination is configurable; that is, you can replace the value of the quote key (') with the value of another key in the RAF configuration file (Section 2). All RAF documentation uses the default ACTION + ' combination.

Terminology

This document uses the following terms:

cluster workstation	any of the following models connected to a server in a cluster configuration: B24, B26, B27, B28, B38, B39, SuperGen Series 1000 (as a Source only), SuperGen Series 2000, SuperGen Series 3000, or SuperGen Series 5000 workstations
server	any of the following models serving as a hub for cluster communication: B26, B27, B28, B38, B39, XE520/XE530, or SuperGen Series 5000
cluster configuration	a local CTOS resource-sharing network consisting of a server connected to cluster workstations
Source workstation	a local workstation that monitors a Target workstation
Target workstation	a remote workstation that is monitored by a Source workstation
session	the process of monitoring or controlling a Target
BNet network	either a classic BNET or BNet II network

Where to Find More Information

For a complete list of CTOS publications and details on how to order manuals, refer to the *CTOS Customer Product Information Catalog and Price List.* The RAF Software Release Announcement (SRA) contains:

- Restrictions and known limitations
- Ordering procedure

The following table lists titles of product information related to RAF. These titles are current at the time of publication but are subject to change.

For more information about	Refer to
ACTION + KEY combinations	*CTOS Remote Access Facility (RAF) Action Key Quick Reference Guide*
CTOS InControl products	*CTOS InControl Overview*
Event generation	*CTOS Local Event Management (LEM) Administration and Programming Guide*
Modem services	*CTOS Modem Service Operations and Programming Guide*
BNet II	*CTOS BNet II Installation, Configuration, and Administration Guide*
BNET	*CTOS BNET Administration and Operations Guide*
Context/Window Manager	*CTOS Context/Window Manager Installation and Configuration Guide*
Error messages	*CTOS Status Codes Reference Manual* and The **Status Code Reporter** Executive command
Device Service	*CTOS Device Service Interface Programming Reference Manual*
Peripheral Extension Module (PEM)	*CTOS Peripheral Extension Module (PEM) Programming Reference Manual*

Section 1
Overview

This section provides an overview of RAF. This section includes information on:

- What RAF is
- How RAF works
- RAF features
- RAF components
- Event generation

Knowing the terms in Table 1-1 will help you understand the information in this section. For other definitions, refer to the Glossary.

Table 1-1. Overview Terms

Term	Definition
Asynchronous Transmission	A data communication methodology in which each information character, or sometimes each word or small block, is individually synchronized, usually by using start and stop elements. Asynchronous transmission is also called start-stop transmission.
LAN	Local Area Network. A localized communications network limited in the geographic area it can serve.
Packet Switched Network	A network in which data is transmitted in units called packets. Messages are split into packets and reassembled at the receiving end of the communications link.
WAN	Wide Area Network. An expanded communications network that has direct or switched connections. In classic BNET, WAN refers to connections by the HDLC, asynchronous, or X.25 media. In BNet II, WAN refers to connections over OSI Transport-WAN.

What Is RAF?

RAF is remote control software that runs over a communications network. RAF allows you to monitor or control another workstation or an application on a workstation.

For example, banks use RAF to monitor remote workstations that tellers use. They troubleshoot using RAF and record teller activities with the Record and Playback features.

You can use RAF on:

- CTOS B25 family of workstations
- SuperGen Series of workstations
- Shared Resource Processors

RAF is a powerful and effective systems management tool, and it is part of the CTOS InControl suite of system management products.

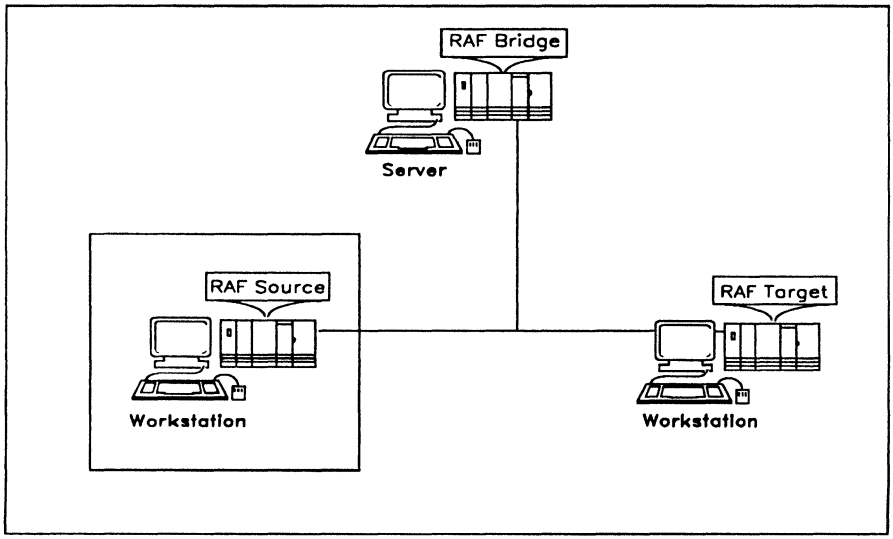
How RAF Works

A workstation, called a *Source*, monitors or controls another workstation or memory partition, called a *Target*. A Source workstation can restrict its activity to simply viewing the activity on a Target, or it can take control of a Target and perform operations on it.

The Source and Target can be part of a CTOS cluster configuration, which typically uses Cluster Local Area Network (LAN) to communicate.

The RAF Source component runs on the Source workstation; while the RAF Target component runs on the Target workstation. The RAF Bridge component transports RAF requests between a server and the target workstations that connect to the server. Figure 1-1 shows these basic RAF components in a typical LAN configuration.

Figure 1-1. Basic RAF Configuration



The following table shows you the networks and their protocols that RAF can run on.

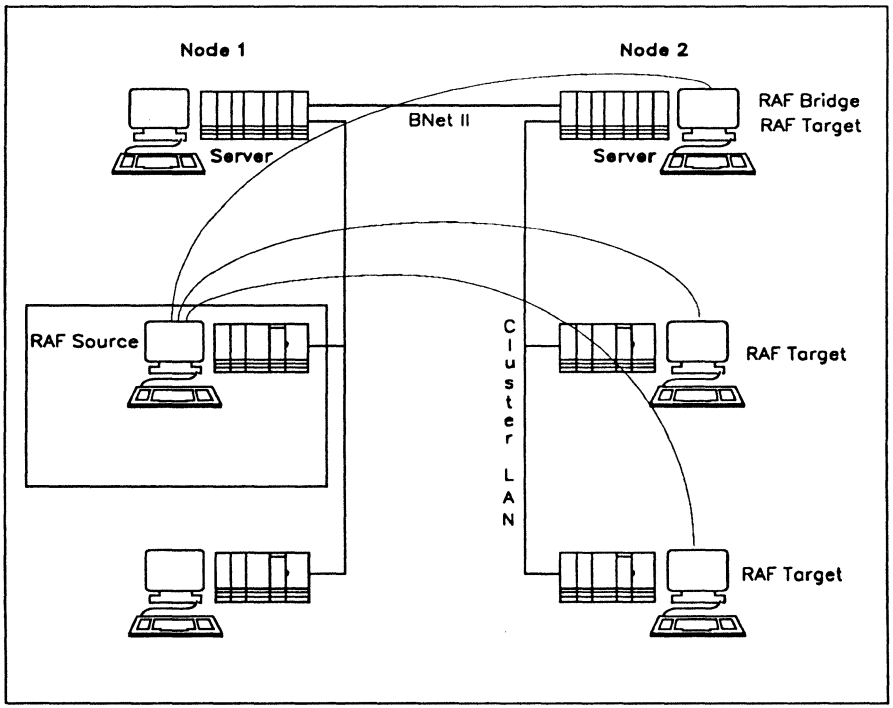
Table 1-2. RAF Networks and Protocols

Network	Communication Protocols
LANs	CTOS Cluster LAN BNET BNet II Modem Service
WANs	Asynchronous Packet switched

With the wide range of networking possibilities, you can use RAF in diverse configurations. You can use RAF when there are two or more workstations that connect over a network.

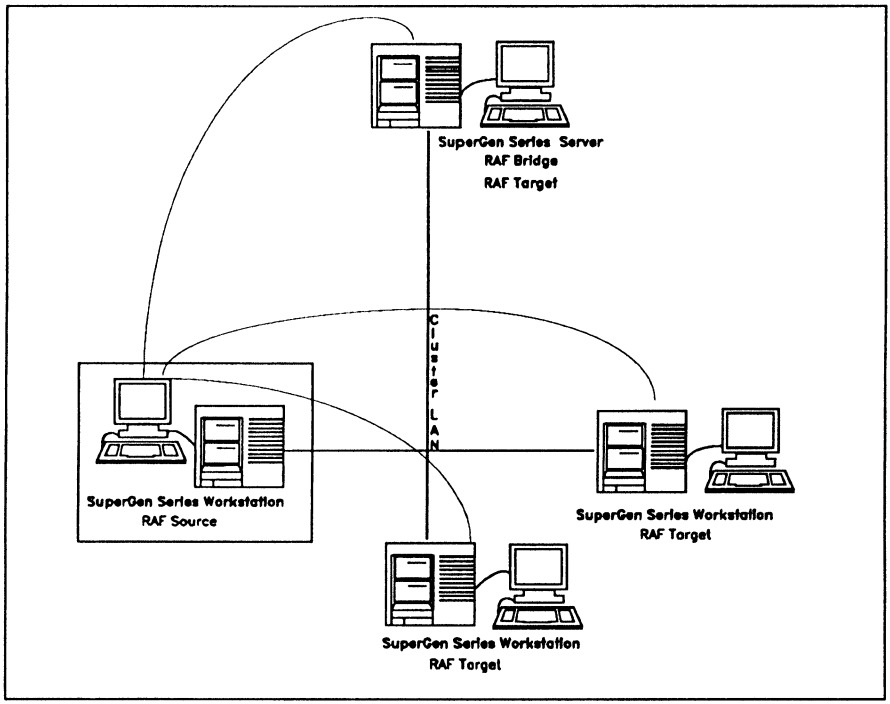
For instance, you can use RAF over a BNet network to control workstations that are clustered to another BNet node. The servers on each cluster have the RAF Bridge service to transport RAF requests from server to Targets; however, a server can also be a Target workstation. Figure 1-2 shows two Cluster LANs that connect using BNet II.

Figure 1-2. Basic RAF Network



You can use RAF with SuperGen Series workstations also that are connected to a SuperGen Series 5000 server. Figure 1-3 shows CTOS SuperGen Series workstations in a network. Section 3 details possible networking configurations.

Figure 1-3. Basic RAF SuperGen Series Network



RAF Features

The following table describes RAF features.

Table 1-3. RAF Features

Feature	Description
Access levels	RAF provides multiple levels of access for each Source user.
Source viewing or control notification	An indicator, V or C, notifies the Target user of monitoring by a Source.
Monitoring detection	A Target user can detect when the Target workstation is monitored and by which Source user.
Monitor inhibitor	A Target user can prevent the viewing or controlling of his or her Target workstation.
File transfer	Files can be transferred between Source and Target workstations, using RAF RS-232 Target interface.
Record and playback	A Source user can record activity on a Target workstation and play back the activity.
Source and Target dialog	Source and Target users can communicate interactively in real time using dialog windows through the RAF Chit-Chat program.
Message posting	Users can send messages to and receive messages from each other.
Remote debugging	A Source user can conduct a debugging session on a Target using the Target's debugger.
Customizeable configuration file	A Source user can customize RAF according to monitoring preferences.
LED keys and beep redirection	A Source user can redirect a Target's LED-equipped keys and beep to the Source workstation.
Mouse redirection	A Source user can redirect a Mouse from the Source to a Target so long as the Source controls the entire Target. ***Note:*** *RAF supports a character-mapped mouse cursor only; you cannot redirect mouse movements in graphical (bit-mapped) applications.*

continued

Table 1-3. RAF Features (cont.)

Feature	Description
Printer redirection	A Source user can redirect a Target's printer output.
MCR device interface	A user can use an MCR Device to log on to RAF Source.
Magnetic Code Reader (MCR) redirection	A Source user can use an MCR device attached to the Source workstation to provide input to applications running on a Target.
RS-232 dial-up connection	A Source user can monitor a Target over a dial-up network.
Configurable video update time interval	The Source screen updates with information from a Target at a user-specified time interval.
Scan capability	A Source user can successively view the screens of Targets in a Cluster LAN or partitions in a single Target.
Configurable keystroke transmission mode	The Source user's keystrokes can be sent interactively or in blocks.
Interactive Performance Monitor (IPM)	A Source user can view the CPU utilization of a Target using the Status option in RAF Source.
Password security	Passwords protect access to Sources and Targets.
Password encryption	A user can use a Peripheral Extension Module (PEM) to encrypt RAF passwords.
Event generation	RAF generates event messages for use with CTOS InControl.
Platform options	You can use RAF on the CTOS B25 family of workstations, the SuperGen Series of workstations, or Shared Resource Processors.
Online Help	RAF incorporates online Help that you display with the **HELP** key.

RAF Components

Table 1-4 presents each RAF component and a brief description.

Table 1-4. RAF Components

Component	Description
RAF Bridge	The system service that receives RAF requests at a Target server and transports them to a Target workstation in a cluster configuration. You load RAF Bridge on the Target cluster server.
RAF Target	The system service that enables the viewing or controlling of the Target workstation.
RAF Source (regular and RS-232)	The component you use to view or control another workstation over a Cluster LAN, BNet network, or a Modem Service network for dial-up connections.
RAF RS-232 Target Interface	The system service that RAF Target uses to communicate with the RAF RS-232 Source over a Modem Service network.
RAF Source User Profile Utility	The utility you use to define the Source user profile and security level.
RAF Target User Profile Utility	The utility you use to define Source users and levels of access to a specific Target.
RAF Screen Recording	The utility you use to record a Target's activity to a file. You replay the file using RAF Source or RAF RS-232 Source.
RAF Query Target ID	The utility you use at a Target to determine its identification number.
RAF Telephone Directory	The component you use to automate dialing into Targets over a Modem Service network.
RAF Script	The component you use to record activity on a Target for later playback.
RAF Query Video Interval	The component you use to determine the frequency with which a Source's screen is updated.
RAF Change Video Interval	The component you use to change the frequency with which a Source's screen is updated.

continued

Table 1-4. RAF Components (cont.)

Component	Description
Performance Gathering Service (PGS)	A system service that gathers data on Target CPU activity. The RAF Source component displays this activity.
Message Posting Bridge	A system service that transports messages in a Cluster LAN. You load Message Posting Bridge on the cluster server.
Message Posting Service	A system service that receives messages at the destination.
Message Posting Notification	The component you use to create, send, save, or recall messages.

Event Generation

Products that are a part of CTOS InControl are capable of generating a special type of system message called an *event message*, or simply an *event*. RAF generates CTOS InControl-compliant events under several conditions, some of which include:

- Successful installation
- Error/Abort conditions
- Deinstallation
- Security violation

For more information on Events generated by RAF components, refer to Appendix D, RAF Events.

Section 2
Installing and Configuring RAF

This section helps administrators install and configure Remote Access Facility (RAF). It describes:

- Preinstall planning
- Installation procedures
- Configuration procedures

Knowing the terms in Table 2-1 will help you understand the information in this section. For other definitions, refer to the Glossary.

Table 2-1. Installation and Configuration Terms

Term	Definition
cluster	A local resource-sharing network that CTOS supports. It consists of a server and one or more client workstations. Communication is by means of the high-speed RS-422 or RS-485 cluster communications channel that is standard on each system.
install	To prepare a software package to run on the computer. This preparation consists of copying programs and data from the installation diskettes and updating system command and request files.
load	To copy a system service from disk to memory for execution.
local system	System on which you are working.
server	Workstation or XE-530, resources of which are shared with client workstations in the cluster.
Source	The local workstation that you use to monitor Target workstations.
Target	The remote workstation that you want the Source workstation to monitor.

Before You Begin

RAF software is supplied on three 5-1/4-inch or 3-1/2-inch write-protected diskettes. Before you install, you should:

- Prepare the installation diskettes
- Determine the installation command that's suitable to your setup
- Determine which RAF components to install

Preparing the Installation Diskettes

You should maintain the installation diskettes by performing the following:

- Do not remove the write-protect labels or use the original diskettes as working copies.
- Use the **Floppy Copy** command to make a copy of each diskette, and install RAF from the copies.
- Store the originals in a safe place.

Determining Which Installation Command to Use

The following chart shows you various CTOS installation commands and which OS version they run on. You should use the **Floppy Install** command if you intend to use CTOS workstations that operate on other software platforms.

You can refer to the *CTOS Executive Reference Manual* for details about the installation commands.

	SOFTWARE INSTALLATION Command	INSTALLATION MANAGER Command	Download RAF From Server onto a Cluster	FLOPPY INSTALL Command	XE SOFTWARE INSTALLATION Command
BTOS II 3.2	✓				
CTOS I 3.3 (real mode)		✓	✓	✓	
CTOS II 3.3 (protected mode)		✓	✓	✓	
CTOS II 3.4 (protected mode)		✓	✓	✓	
CTOS III 1.1 (v series)		✓	✓	✓	
CTOS/XE 3.0					✓

Determining Which RAF Components to Install

You can select RAF components to install. The following table tells you which diskette to begin installation with to install your selected component only.

Table 2-2. RAF Services Diskette Selection

To install...	Begin installation with...
RAF Source RAF RS-232 Source	First diskette
RAF Target	Second diskette
Message Posting	First or second diskette

If you want to install Message Posting only, begin installing either Source or Target and select the Message Posting option.

Modem Service with RAF

If you intend to use a modem with RAF, you need to install the Modem Service software.

If Modem Service software came with your BNet software, install the associated Modem Service files on the BNet installation diskettes; otherwise, install the Modem Service packaged with RAF.

> **Caution:**
>
> If you use Software Distribution (SWD) to install RAF remotely, exercise caution; if the RAF installation fails, you may be unable to use RAF to correct the problem.

Installing RAF

Use the following procedures to install RAF from the installation diskettes to your hard disk.

Installing RAF on BTOS, CTOS, AND CTOS/XE Systems

The following procedure provides installation steps for:

- BTOS II 3.2
- CTOS I 3.3.1 (real mode)
- CTOS II 3.3.1 (protected mode)
- CTOS II 3.4 (protected mode)
- CTOS III 1.1 (v series)
- CTOS/XE 3.0 or higher

The procedure does not describe details of installation operations. Consult your CTOS Executive documentation for installation process details.

Use the following procedure to install RAF onto your system:

1. Type one of the following Executive commands to start the installation process; then press GO:
   - **Installation Manager**
   - **Software Installation**
   - **Floppy Installation**
   - **XE Software Installation**
2. Choose one of the following:
   - If you are using **Installation Manager** and are installing onto a local workstation, when the system prompts you:

     select **Install New Software**; then press **GO**.

     select **Floppy Installation**; then press **GO**.

     select **Continue Installation**; then press **GO**.
   - If you are using **Installation Manager** and are installing onto a server from which clusters can install RAF, when the system prompts you:

     select **Install New Software**; then press **GO**.

     select **Floppy Installation**; then press **GO**.

     select **Examine/Change Defaults**; then press **GO**.

     select **Yes** for the Public Parameter; then press **GO**.
   - If you are using any of the other installation commands, go to Step 3.
3. Follow the instructions on your screen.
4. When installation is complete, remove the diskette from drive F0 and store it and the other diskettes in a safe place.

When you complete installation, reboot the system.

Installing RAF from a Server

This subsection tells you how to download RAF from a server and install it on a cluster workstation.

Note: *If you want to download Message Posting only, start installing either Source or Target, then select the Message Posting option.*

Use the following procedure if you want to download RAF software from the server:

1. Type **Installation Manager** at the Executive command line; then press **GO**.
2. When the system prompts you:

   Select **Install New Software**; then press **GO**.

   Select **Install From Server**; then press **GO**.

   Select **Continue Installation**; then press **GO**.
3. When the system displays the list of public software, select **RAF Source** or **RAF Target**; then press **GO**.

   Note: *When using Installation Manager to download software from a server, you can select one software component only from the list.*
4. When installation is complete, press **FINISH**.

When you complete installation, reboot your system.

Configuring RAF

To set parameters, RAF uses a default configuration file, *RAFConfig.sys*, that you installed when you installed RAF onto hard disk.

You can edit *RAFConfig.sys* to customize RAF to your environment. Table 2-3 defines the parameters in the file.

Table 2-3. RAF Configuration File Parameters

Parameter	Description
:SourceTimeOut:	Specifies the length of time, in minutes, that can elapse with no keyboard input at the Source workstation, after which RAF ends a View or Control session. Range: 1 to 180 Default: 30
:ActionQuote:	Use this parameter to direct ACTION key input to CTOS. (Normally, RAF interprets ACTION key entries as RAF input.) Enter the value of the Action quote. Default: 39 decimal, the quote key (') ***Note:*** *RAF documentation uses the default.*
:RS232TimeOut:	Specifies the length of time, in seconds, that can elapse with no message traffic (including system messages) between a RAF RS-232 Source and Target before RAF disconnects. If you have a Target that is a BNet Target, you should set this parameter to be 10 seconds greater than the BNet timeout parameter. Range: 6 to 60 Default: 10
:BlockKeysTimeout:	If transmitting keystrokes in block mode, specifies the length of time, in seconds, between transmissions of blocks of keystrokes to a Target. Range: 2 to 10 Default: 3
:NoOfSendKeys:	Specifies the number of Send Key requests to keep pending. If you are using a Target Editor or a word processor, you can increase the value of this parameter to improve system performance. Range: 2 to 5 Default: 3

continued

Table 2-3. RAF Configuration File Parameters (cont.)

Parameter	Description
:SzVidUpdateBuffer:	Specifies the size, in bytes, of the buffer used to send video updates from the Target to the Source. Range: 256 to 1024 Default: 1024
:Notification:	Specifies the notification type. You can enter either No, Audio, or Visual. Default: No
:NotifyBlink:	Specifies a blinking or steady Visual notification. You can enter either Yes or No. Default: No (steady notification)
:WrapLogFileAllowed:	Specifies whether or not RAF overwrites previous entries in the log file when the log file is full. You specify Yes to allow RAF to overwrite entries in the log file, beginning with the oldest. If you specify No and the log file on a Target becomes full, you cannot access that Target until you reset the parameter to Yes, then unload and reload the Target or delete the log file and recreate it. Default: No

Section 3
Configuring RAF Networks

This section describes communication networks and how RAF functions within them.

Note: *The network configurations shown in the figures in this section are intended as examples only. Your network configuration need not be limited to the examples.*

Knowing the terms in Table 3-1 will help you understand the information in this section. For other definitions, refer to the Glossary.

Table 3-1. Networking Terms

Term	Definition
BNA	Burroughs Network Architecture. A proprietary network architecture that provides lower OSI layer services, including specialized features and functionality.
BNet node	A workstation (standalone, server, or cluster with a local file system) or an SRP on which the BNet services have been loaded, and which has been configured to communicate with one or more other nodes in the network.
Cluster access	A feature whereby reduced-size versions of the Net Agent and Net Server provide complete BNet II functionality to workstations communicating by means of the RS-422 and RS-485 cluster lines only.
DCA	Distributed Communications Architecture. A Unisys proprietary network architecture that provides lower OSI layer services.
Network	Two or more workstations, connected by cables or telephone lines.
OSI	Open Systems Interconnect. A set of standards that provides consistent hardware and software interfaces among various network products.

continued

Table 3-1. Networking Terms (cont.)

Term	Definition
OSI Transport-LAN	The Unisys version of a LAN that BNet II uses.
Protocol	A set of rules by which computers communicate.
SNA	Systems Network Architecture. A transport service that is proprietary to IBM.
X.25	A packet-switched network protocol based on a standard developed by the International Telegraph and Telephone Consultative Committee (CCITT).

RAF Networks

The following table shows the four types of Local Area Networks (LANs) that RAF uses.

Table 3-2. RAF Networks

Type	Description
CTOS Cluster LAN	RAF uses this networking capability that's built in to the CTOS operating system to communicate over a cluster LAN.
BNet II	The communications package that enables CTOS users to access either local or remote files and resources of other systems that are on another BNet node. BNet II communicates via BNET Transport, which provides access to the Open Systems Interconnection (OSI) transport services.
BNET	Commonly referred to as classic BNET since it is the precursor to BNet II; BNET provides communication services between Cluster LANs, but does not provide access to OSI services. ***Note:*** *RAF does not use BNET to access Targets that are Cluster Access nodes.*
Modem Service	The service that provides asynchronous dial-up connections over telephone lines and direct cable connections through a null-modem cable; Modem Service is the transport media that the RS-232 Target Interface Service uses.

Figure 3-1 shows a BNet II network that connects cluster LANs.

Figure 3-2 shows a Modem Service network that connects two Cluster LANs.

Figure 3-1. BNet II Network Connecting Cluster LANs

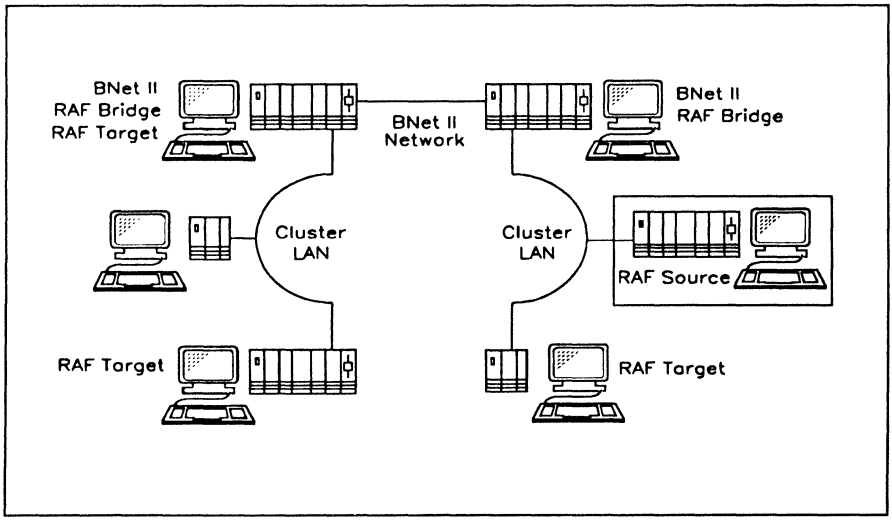


Figure 3-2. Modem Service Network

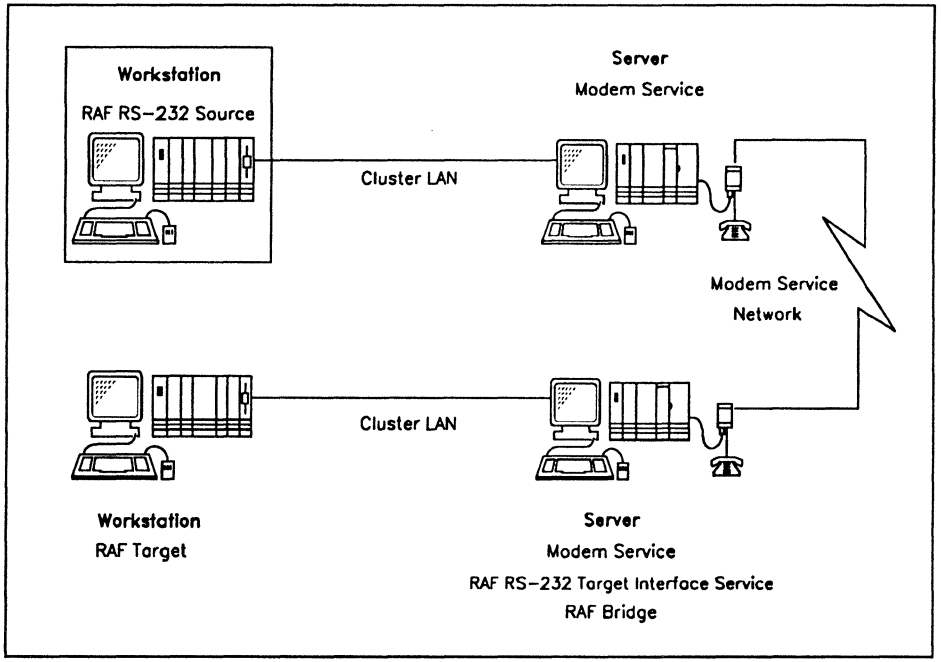


Figure 3-3 shows all four networks and an extended view of a BNet network. Figure 3-4 shows the same networks and an extended view of a BNet II network. These figures do not depict actual BNet components, rather, they depict the types of networks BNet makes available to its users.

Figure 3-3. Supported Networks and Extended BNET Network

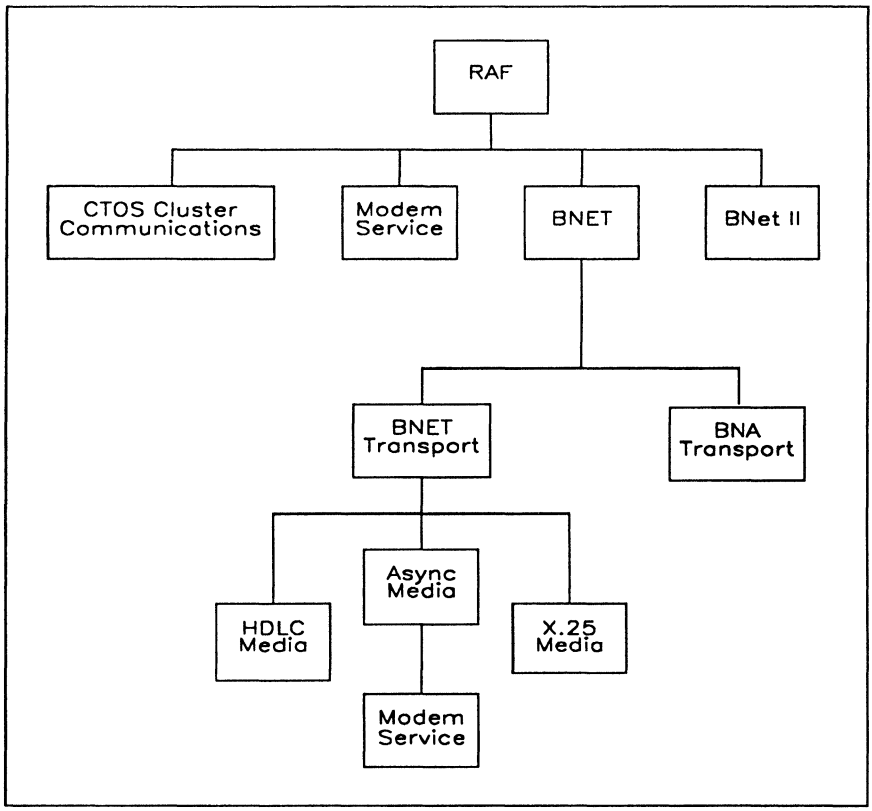
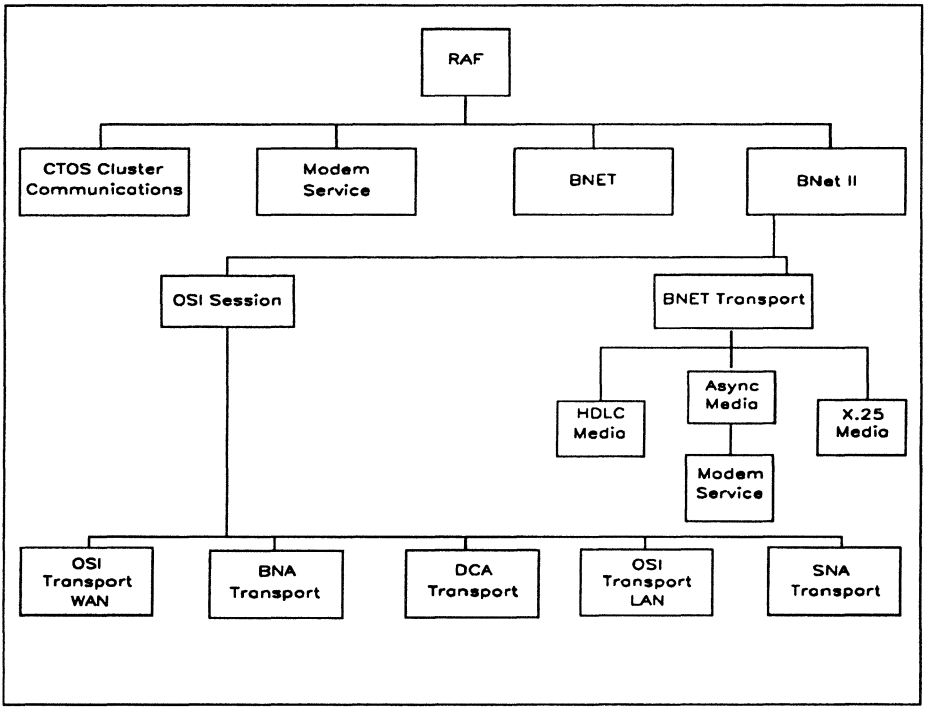


Figure 3-4. Supported Networks and Extended BNet II Network

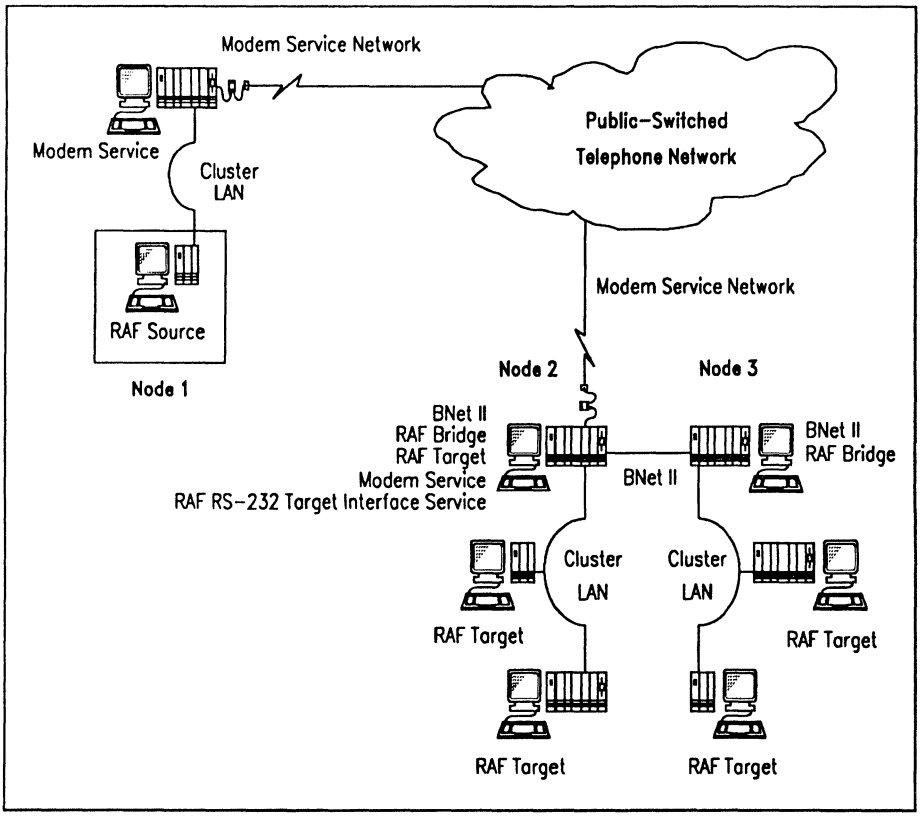


Local and Wide Area Networks

RAF can run on an Open Systems Interconnection (OSI) network. Token Ring and Ethernet LANs are accessed through the OSI Session and OSI Transport LAN Layers of BNet II.

Modem Service can also provide access to a Wide Area Network (WAN) through its dial-up capability. Figure 3-5 shows RAF running over a Modem Service WAN.

Figure 3-5. Modem Service Wide Area Network



RAF can run over a Modem Service WAN or RAF can use a packet-switched (X.25) network, which it accesses through the OSI Session and OSI Transport WAN services of BNet II.

The number of LANs and WANs that RAF runs on makes it possible, for example, for a RAF Source located in New York to monitor a RAF Target located in Los Angeles, using either Modem Service's dial-up capability, BNET, or packet-switched networks.

Unisys Mainframe Connectivity

RAF can run on networks connecting workstations to a Unisys mainframe using the BNA communications protocol. Figure 3-6 shows two Cluster nodes connected with BNET and BNA through an A or V Series host. Figure 3-7 shows two cluster nodes connected by BNet II through an 1100 or 2200 Series host.

Figure 3-6. Unisys A/V Series Mainframe Connectivity

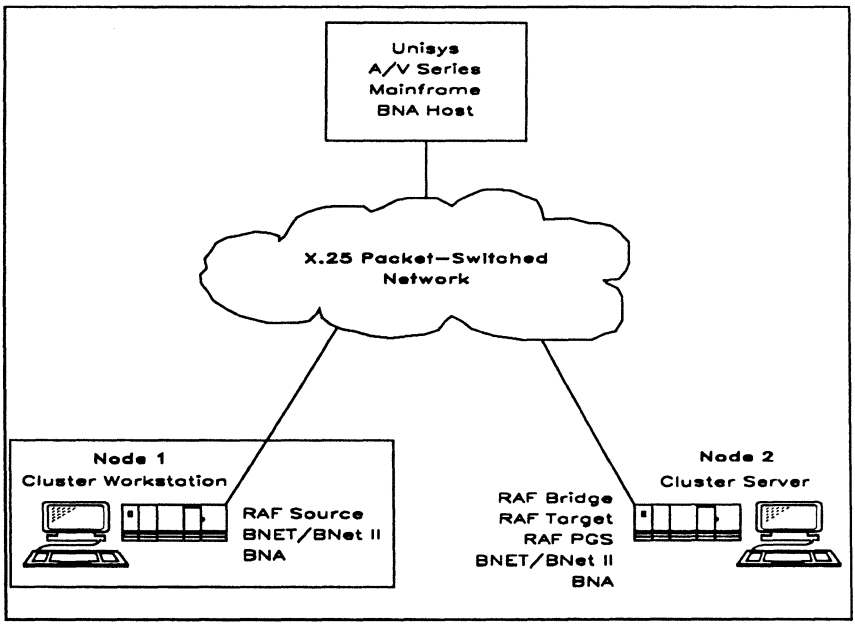
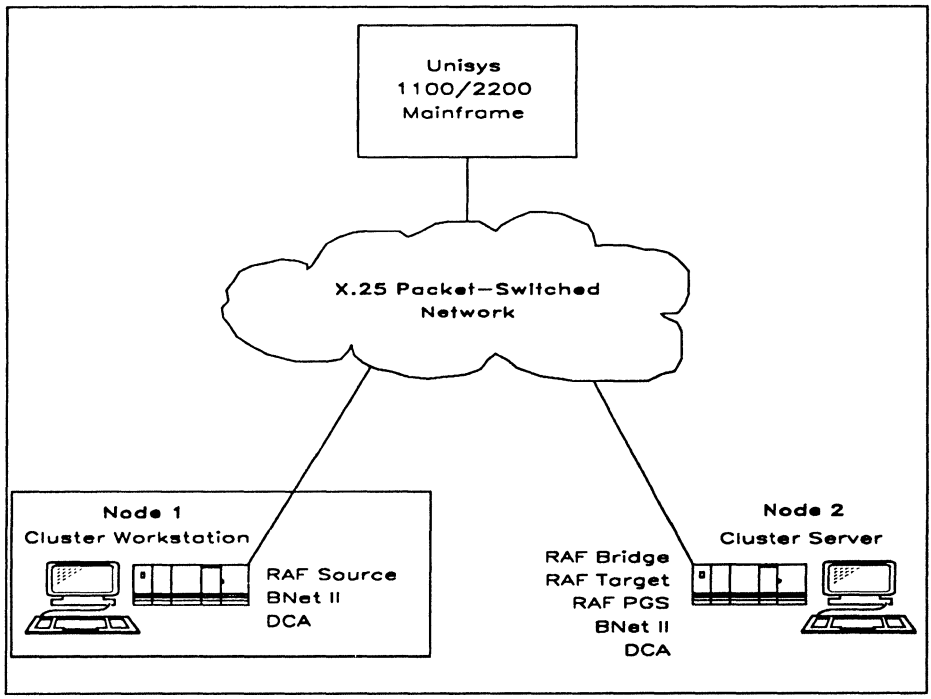


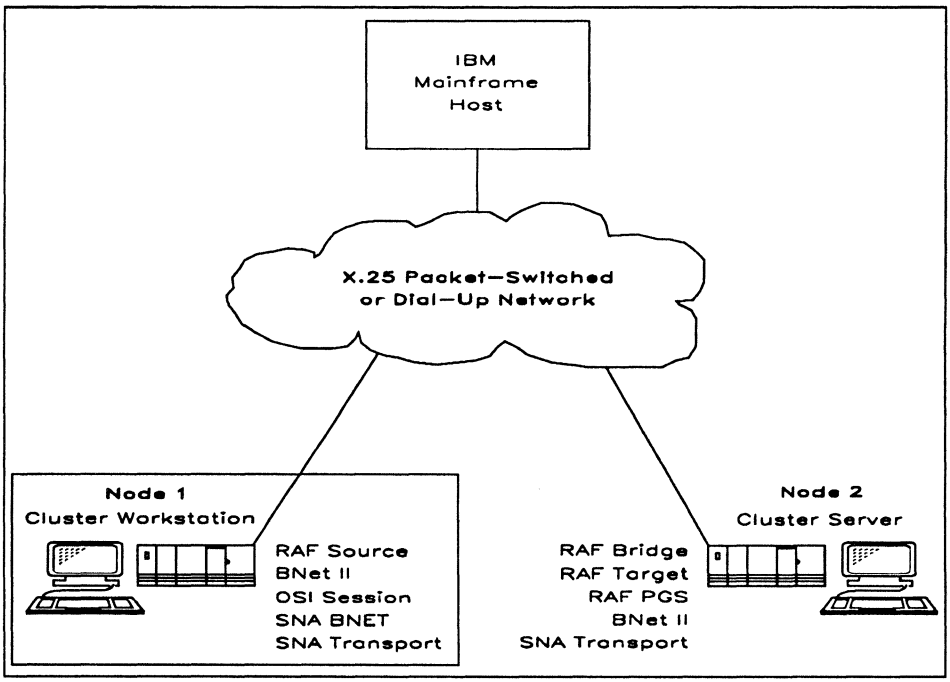
Figure 3-7. Unisys 1100/2200 Series Mainframe Connectivity



IBM SNA Connectivity

RAF can also be used between workstations connected to an IBM host. Figure 3-8 shows two cluster nodes connected with BNet II, OSI Session, SNA BNet, and SNA Transport, which provide the connection through either X.25 or dial-up lines. Node 1 can control Node 2 through each node's connection to the IBM mainframe.

Figure 3-8. IBM SNA Connectivity



Which RAF Components to Use

Table 3-3 shows the key RAF components, where they are loaded, and the networks they use.

Table 3-3. Which RAF Components to Use

	Source Workstation	Target Workstation	Server on Source Workstation's Cluster LAN	Server on Target Workstation's Cluster LAN
Cluster LAN	RAF Source	RAF Target PGS (Optional)		RAF Bridge
BNET or BNet II	RAF Source	RAF Target PGS (Optional)	BNET or BNet II	BNET or BNet II RAF Bridge
Modem Service	RAF RS-232 Source Modem Service[1]	RAF Target PGS (Optional) RS-232 Target Interface Service[2] Modem Service	Modem Service[1]	RAF Bridge RS-232 Target Interface Service[2] Modem Service

1 Modem Service can be loaded at either Source workstation or Source server.

2 On workstations that have a modem or direct RS-232 connections, you need to load both RAF RS-232 Target Interface Service and Modem Service.

Note: *RAF Bridge is required when a workstation in a Cluster LAN has RAF Target installed and loaded.*

Documenting Your Network Configuration

Appendix B provides a component worksheet that you may find helpful to document your network configuration. You should document:

- Identification of each workstation and server
- Software installed on each workstation and server
- Software memory requirements
- Type of network configuration (Cluster LAN, BNET, BNet II, or Modem Service)
- Network location of each workstation and server

Section 4
Customizing the RAF Environment

This section contains information on:

- Defining Source and Target user profiles
- Defining and managing users
- Defining security levels
- Creating and using a script file

What Are Source and Target User Profiles?

A RAF Source user profile defines a user's access to RAF Source. Likewise, a RAF Target user profile defines access to a Target workstation.

System Administrators create the RAF Source profiles with the RAF Source User Profile utility. They create the RAF Target profiles with the RAF Target User Profile utility, as shown in Table 4-1.

Note: *If no Administrator is defined, any user can create, modify, or delete RAF user profiles.*

Table 4-1. Profile Utilities

Utility	Purpose	Location
RAF Source User Profile utility	Enabling security and defining RAF Source user profiles and MCR profiles	Source workstation
RAF Target User Profile utility	Enabling security and defining RAF Target user profiles, Source user access levels, and workstation identifications	Target workstation or server

You use the RAF Source User Profile utility to define the following information:

- For each Source user: name, password, encryption and file transfer status.
- Magnetic card reader (MCR) Profile allowing users to log on with magnetic cards. The MCR Profile contains information about the location of the user name and password on the card's magnetic strip.

You use the RAF Target User Profile utility to define the following information:

- For each Target workstation: Source user name, password, and access level.
- Name and size of the log file to which RAF Target writes information.

If you do not specify a Target name when you load RAF Target, RAF uses the defaults in the *RAFTargetProfile.Sys* file. If you enter a unique workstation identifier when you load RAF Target, RAF prefixes the Target profile name with that workstation identifier. For example, if you enter **Teller** as the Target name, RAF uses *TellerTargetProfile.Sys*.

Note: *If RAF services are already loaded, additions or changes to RAF configurations or user profiles do not take effect until you unload RAF services and reload them.*

Security

RAF security can be enabled or disabled. You enable or disable security in the RAF Source profile and the RAF Target profile.

If you enable security, you must enter a user name and password that match a user name and password in the RAF Source profile and RAF Target profile. Your security level determines your access to RAF features.

If you disable security, then RAF does not check for passwords or security levels and users can access all RAF features, provided they enter valid user names.

You can use the RAF configuration file to enable and disable RAF Target security.

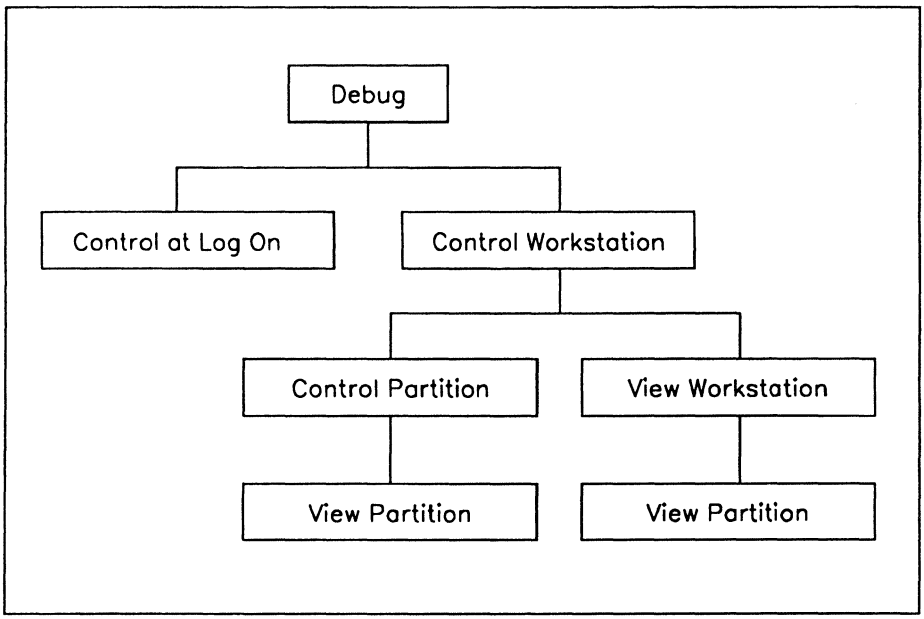
Security Hierarchy

RAF security is arranged in a hierarchical structure; if a Source user is allowed to perform a function, that Source user can also perform all functions below that one in the hierarchy. For example, if RAF allows a Source user to access the Target for debugging, then it allows that user to control and view the Target. On the other hand, if a Source user has view privileges only, then RAF denies access when the user tries to control a workstation.

A Source user that does not have Debug privileges, may have Control Workstation or Control at Logon privileges, but not both. Control at Logon privilege, allows a Source user to access a Target only when that Target is at the signon screen.

One user can have different levels of access to different nodes. The security hierarchy is valid for access to RAF Targets only. Figure 4-1 shows this security hierarchy.

Figure 4-1. Security Hierarchy



Creating and Modifying Source User Profiles

Use the following procedures to create or modify a Source user profile.

Signing on to the Source User Profile Utility

1. Type **RAF Source User Profile** on the Executive command line; then press **GO**.

   The RAF Source User Profile Log On screen shown in Figure 4-2 displays.

2. Enter the administrator name; then press **RETURN**.
3. Enter the administrator password.

The default administrator name is ADMIN and the default administrator password is ADMIN.

After you enter the administrator name and password, you use the function keys to select tasks as described in Table 4-2.

Figure 4-2. Source User Profile Log On Screen

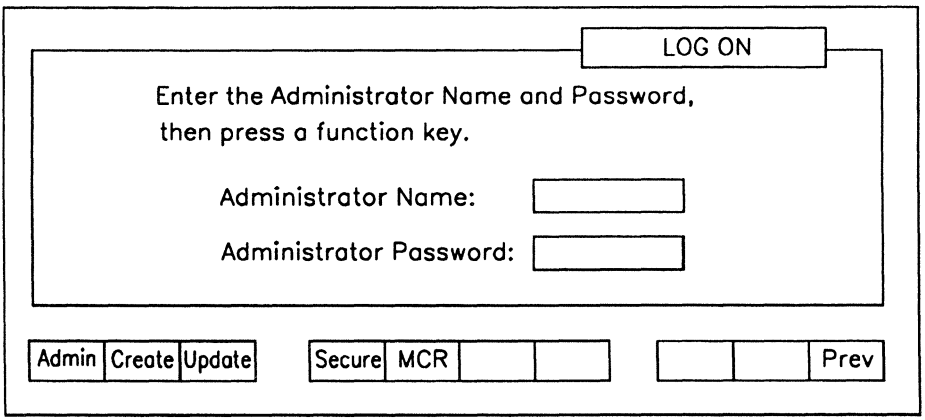


Table 4-2. Source User Profile Logon Function Keys

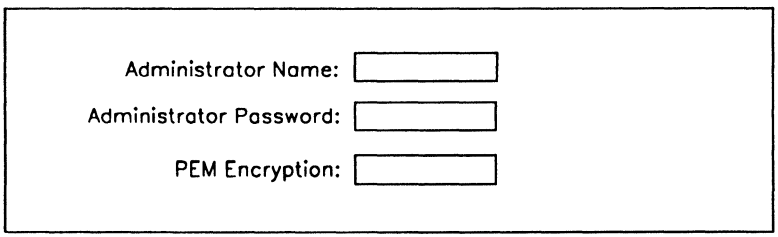
Key	Description
F1	Change the Source administrator name, password, or encryption status
F2	Create a new Source user profile
F3	Modify a Source user profile
F4	Enable and disable RAF security
	When security is enabled, the F4 key is highlighted and Source users without passwords cannot log on
F5	Create an MCR Profile
F10	Exit the program

Changing the Administrator Name, Password, or Encryption Status

Use the following procedure to change the Source administrator name, password, or encryption status.

1. At the RAF Source User Profile Log On screen, press **Admin (F1)**.

   The Source User Profile Administration form displays:



2. Enter the new administrator name and password.
3. To encrypt the Administrator password using a PEM device, type **Yes** in the *PEM Encryption* field; then press **GO**.

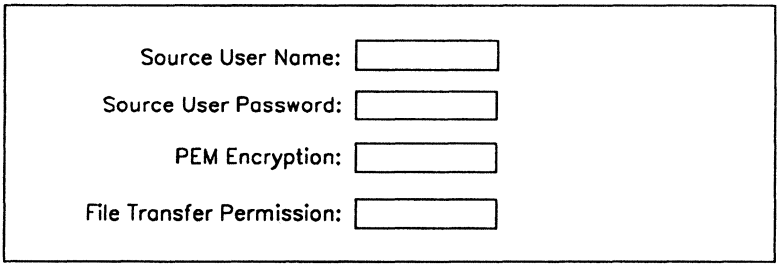
Refer to Encrypting RAF Passwords in this section for more information on Peripheral Extension Module (PEM) encryption.

Creating a Source User Profile

You create a Source user profile for each Source user. Use the following procedure to create a Source user profile:

1. Press **Create (F2)** on the RAF Source User Profile Log On Screen,

   The Create Profile menu displays.



2. Enter the Source user name and password.
3. To encrypt the Source User's password using a PEM device, type **Yes** in the *PEM Encryption* field.
4. To allow the user to transfer files, enter **Yes** in the *File Transfer Permission* field then press **GO**.

After the utility creates the user profile, the RAF Source Profile Log On screen redisplays.

Refer to Encrypting RAF Passwords in this section for more information on PEM encryption.

Modifying or Deleting Source User Profiles

Use the following procedure to modify or delete one or more Source user profiles:

1. Press **Update (F3)** at the RAF Source Profile Log On Screen.

   RAF displays a list of user profiles.

2. Move the cursor to the Source User name that you want to update or delete.

3. Choose one of the following:

   - To delete a user profile, press **Delete (F1)**.
   - To modify a user profile, press **Modify (F2)**. Edit the displayed information; then press **GO**.
   - To delete all user profiles, press **DelAll (F3)**.

Enabling and Disabling Security

If you enable security, no Source user can log on without a password.

You press the **Secure (F4)** function key to enable and disable RAF security. If security is enabled, the **Secure (F4)** function key is highlighted. If it is not enabled, the key displays in normal video mode.

Creating a Magnetic Card Reader (MCR) Profile

You create an MCR Profile to enable Source users to sign onto RAF using magnetic-strip cards. The MCR Profile defines the location of the user name and password information on the magnetic strip.

Use the following procedure to create an MCR Profile:

1. Press **MCR (F5)** on the RAF Source Log On Screen.

   The MCR Profile form shown in Figure 4-3 displays. Refer to Table 4-3 for a description of each parameter.

2. Enter values for each parameter; then press **GO**.

Figure 4-3. Source User MCR Profile Form

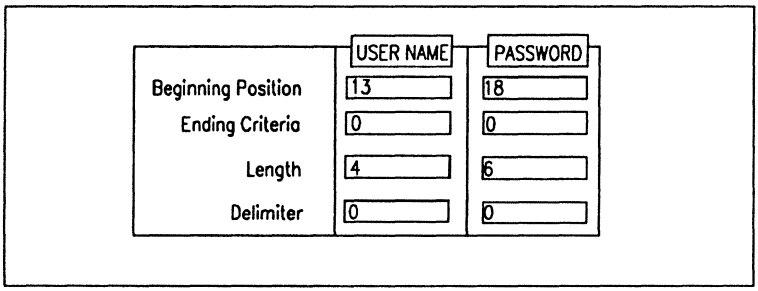


Table 4-3. MCR Profile Parameters

Parameter	Description
Beginning Position	The position of the first number or character of the user name and password on the magnetic card The first number or character on a magnetic card strip has the beginning position 0.
Ending Criteria	The ending criteria of the user name and password Possible values 0 = fixed-length number 1 = variable-length number
Length	The length of the user name or password This value represents 1 or more characters. Use this for fixed-length fields only.
Delimiter	The ASCII equivalent of the delimiter character RAF scans the data from the magnetic card strip from the Beginning Position to the Delimiter character you specify. That data represents the user name and password. Use for variable-size fields only.

In the following example, the contents of an MCR card are shown on the first line, and their relative position on the second line:

```
Contents: 4401210203235John/110912/BofXYZ
Position: 00000000001111111111222222222 3
          0123456789012345678901234567890
```

In this example, the user name is John, starting at position 13, and the password is 110912, starting at position 18. The delimiter is the "/" character (ASCII value 47). Table 4-4 shows the values for configuring the user name and password in the example as fixed-length entities. Table 4-5 shows the values for configuring the user name as fixed-length and the password as variable-length.

Table 4-4. MCR Profile Example With Fixed-Length Password

Parameter	User Name	Password
Beginning Position	13	18
Ending Criteria	0	0
Length	4	6
Delimiter	-	-

Table 4-5. MCR Profile Example With Variable-Length Password

Parameter	User Name	Password
Beginning Position	13	18
Ending Criteria	0	1
Length	4	-
Delimiter	-	47

Creating Target User Profiles

You create Target user profiles at the Target workstation. Use the following procedures to create a Target user profile.

Signing on to the Target User Profile Utility

1. Type **RAF Target User Profile** on the Executive command line; then press **RETURN**.

   The following command form displays:

```
RAF Target User Profile
   [Workstation ID (Default = "RAF")]
```

2. Enter a unique workstation ID (optional); then press **GO**.

   RAF attaches the workstation ID to the beginning of the file name, *TargetProfile.Sys*. For example, if you enter **Teller**, RAF creates or opens the Target profile in *TellerTargetProfile.Sys*.

3. Enter the administrator name and password.

The default administrator name is ADMIN and the default administrator password is ADMIN.

After you enter the administrator name and password, you use the function keys to select tasks as described in Table 4-6.

Table 4-6. Target User Profile Logon Function Keys

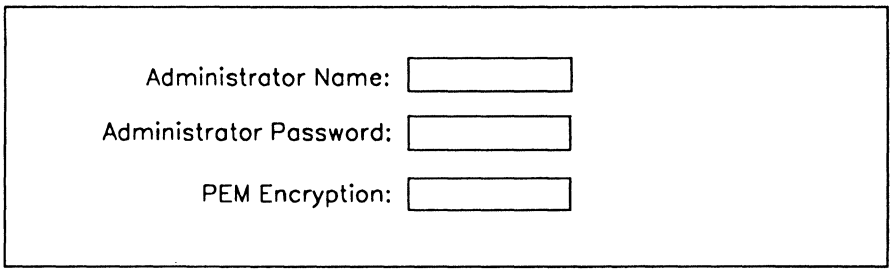
Key	Description
F1	Change the Target administrator name, password, or encryption status
F2	Create a new Target user profile
F3	Modify a Target user profile
F4	Enable and disable RAF security
	When security is enabled, the F4 key is highlighted and Target users without passwords cannot log on.
F5	Define a log file
F6	Allow user to prevent monitoring of the workstation
F10	Exit from the program

Changing the Administrator Name, Password, or Encryption Status

Use the following procedure to change the Target administrator name, password, or encryption status.

1. At the RAF Target User Profile Log On screen, press **Admin (F1)**.

   The Target User Profile Administration form displays:



2. Enter the new administrator name and password.
3. To encrypt the Administrator password using a PEM device, type **Yes** in the *PEM Encryption* field.
4. Press **GO**.

Creating a Target User Profile

You create a Target user profile for each Source user who can access this Target. Use the following procedure to create a Target user profile:

1. Press **Create (F2)** on the RAF Target User Profile Log On Screen,

   The Create Target Profile window shown in Figure 4-4 displays.

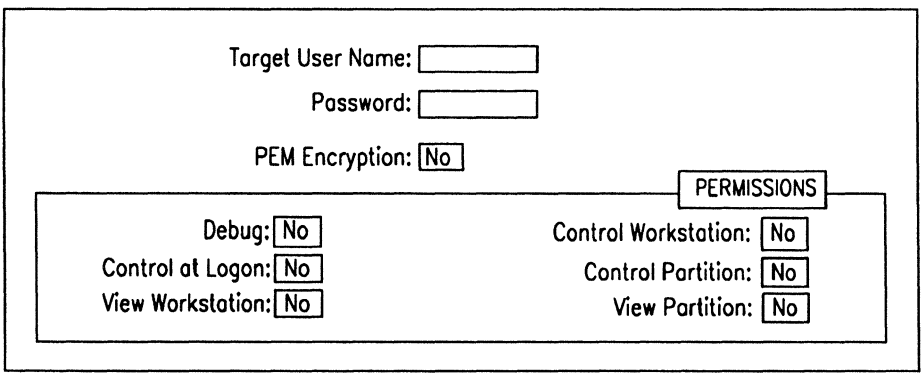
2. Enter the user name and password of a Source user who is to have access to this Target.
3. To encrypt the Target user's password using a PEM device, type **Yes** in the *PEM Encryption* field.
4. Enter **Yes** or **No** in each of the Permissions fields to specify which privileges the Source user should have; then press **GO**.

After the utility creates the New User profile, the RAF Target Profile Log On screen redisplays.

Refer to Encrypting RAF Passwords in this section for more information on PEM encryption.

Note: *If you select a combination of access privileges not consistent with RAF's security hierarchy, RAF overrides your selections.*

Figure 4-4. Create Target Profile Window



Modifying or Deleting Target User Profiles

Use the following procedure to modify or delete one or more Target user profiles:

1. Press **Update (F3)** at the RAF Target Profile Log On Screen.

   RAF displays a list of user profiles.

2. Move the cursor to the Target User name you want to update or delete.

3. Choose one of the following:

   - To delete a user profile, press **Delete (F1)**.
   - To modify a user profile, press **Modify (F2)**.

     RAF displays the selected user's profile. Edit the information in the fields; then press **GO**.

   - To delete all user profiles, press **DelAll (F3)**.

Enabling and Disabling Target Security

If you enable security on a Target, a Source user cannot log on without a password.

You press the **Secure (F4)** function key to enable and disable RAF security. If security is enabled, the **Secure (F4)** function key is highlighted. If it is not enabled, the key displays in normal video mode.

Defining a Log File

Use the following procedure to define the Target log file:

1. Press **LogDef (F5)** on the RAF Target User Profile Log On screen, press.

   The Log File Definition form displays.

2. Type in the maximum log file size in sectors and the log file name; then press either **GO** or **Save (F1)**.

Setting Source Monitoring Privileges

If a Target user does not have the privilege of preventing Sources from monitoring his or her Target, the **DisSrc (F6)** function key is highlighted.

You press the **DisSrc (F6)** function key to enable and disable RAF security. If security is enabled, the **DisSrc (F6)** function key is highlighted. If it is not enabled, the key displays in normal video mode.

Encrypting RAF Passwords

If you have a PEM equipped with a Data Encryption Standard (DES) chip, you can encrypt RAF passwords.

Note: *If the RAF Source has PEM encrypted passwords, the Target must have PEM encryption capability. The user name and password in a user's Source user profile should match the user name and password in his or her Target user profile.*

Follow the procedures in your PEM encryption documentation to create a master key.

After you have defined the master key, refer to Creating a Source Profile and Creating a Target Profile in this Section for procedures for setting the *PEM Encryption* and *User Password* fields to **Yes** in your RAF Source and RAF Target user profiles.

Script Files

The Script File utility allows you to create files that automatically establish a connection with a Target when you invoke RAF Source or RAF RS-232 Source.

Creating a Script File

Use the following procedure to create a script file:

1. Type **RAF Script** on the Executive command line on a Source workstation; then press **RETURN**.
2. Enter a name for the script file you want to create in the *ScriptFile* parameter; then press **GO**.

   Note: *You may find it helpful to give the script file a name descriptive of the Target you will reach.*

   The Script File window displays. Refer to Table 4-7 for descriptions of the parameters of the Script File command form.
4. Type in the necessary information in each field of the Script File window; then press **GO**.
5. Choose one of the following:
   - Press **GO** to save the information and exit the utility.
   - Press **FINISH** to exit the utility without saving.
   - Press **CANCEL** to continue editing the information.

RAF creates the script file.

Some of the script file parameters refer to Telephone Directory entries. Refer to Configuring a RAF Telephone Directory (Section 5) for more information.

The Telephone Directory and Channel parameters apply to RAF RS-232 Source only.

Table 4-7. Script File Window Parameters

Parameter	Description
MCR Input	Enter **Yes** if the user is to use the MCR for supplying user name and password.
User Name	Enter the name of the Source user who will use this script file.
Password	Enter the password of the Source user who will use this script file.
Telephone Directory Entry	If you created a Telephone Directory entry for the Target this script will access, enter the name of the entry.
Channel	Enter the channel (serial port) to which your modem is connected. Refer to Appendix C for a list of channel identifiers.
Telephone Number	If you created a Telephone Directory entry for the Target this script will access, enter the phone number.
Node	If this script will access a Target on a BNet node, enter the node name.
Workstation	Enter the workstation identifier of the Target you want to access.
Mode	Enter the type of monitoring you want to perform on the Target. Choose one of the following: 0 = control entire workstation 1 = view entire workstation 2 = control one partition 3 = view one partition
Partition	To view or control a single partition on the Target, enter the partition identifier. For example, enter **CM01** for the first Context Manager application partition, **CM02** for the second, and so on.
Printer Redirection	To redirect printer output from the Target to the Source, enter **Yes**.

Using the Script File

To use a script file, enter the script file name on the *[ScriptFile]* parameter of the **RAF Source** or **RAF RS-232 Source** Executive command form. RAF automatically performs the steps required for logging onto RAF Source and establishing a connection based upon the contents of the script file. If the *MCR Input* parameter is **Yes**, RAF pauses the script and waits for you to swipe your card through the MCR.

Refer to Managing a Distributed Environment with RAF (Section 7) for more information on the **RAF Source** and **RAF RS-232 Source** commands.

Section 5
Configuring a RAF Telephone Directory

The Telephone Directory is a helpful tool to use with RAF RS-232 Source. The Telephone Directory contains a list of Targets and their telephone numbers that automatically display on the Dial-Up Menu when you start the RAF RS-232 Source program.

This section contains information on:

- Creating a Telephone Directory entry
- Modifying or deleting Telephone Directory entries
- Exiting from the Telephone Directory
- Using the Telephone Directory

Creating a Telephone Directory Entry

Use the following procedure to create a telephone directory entry:

1. At the Executive command line, type **RAF Telephone Directory**; then press **GO**.

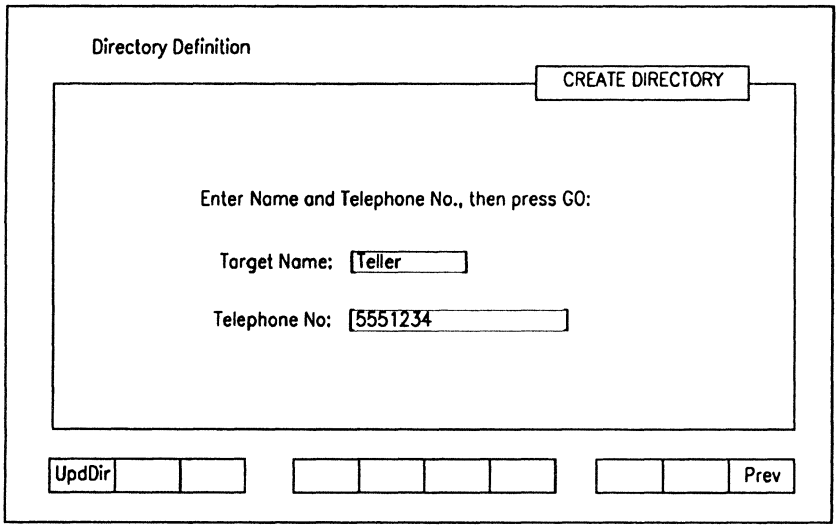
   The Create Directory screen displays (refer to Figure 5-1).

2. Type the name of the Target in the *Target Name:* field; then press **RETURN**.

3. Type the telephone number you use to access the Target in the *Telephone No:* field; then press **GO**.

   RAF adds the entry to your Telephone Directory.

Figure 5-1. Create Directory Screen



Modifying or Deleting Telephone Directory Entries

Use the following procedure to modify or delete an entry in the Telephone Directory:

1. At the Create Directory screen, press **UPDDIR (F1)**.

   The Update Directory screen displays, as shown in Figure 5-2.

2. Move the cursor to the entry you want to modify or delete.

   When you select a entry, it becomes highlighted.

3. Choose one of the following:

   - To delete the telephone entry, press **Delete (F1)**

     RAF deletes the entry.

   - To modify the telephone entry, press **Modify (F2)**

     The Modify Directory screen appears (refer to Figure 5-3).

     - To change the name of the entry, enter the new name in the *Name:* field.
     - To change the phone number, enter the new number in the *Telephone No:* field.
     - To return to the Update Directory screen, press **GO**.

   - To delete all telephone entries, press **DelAll (F3)**

     RAF deletes all the entries in the Telephone Directory.

Figure 5-2. Update Directory Screen

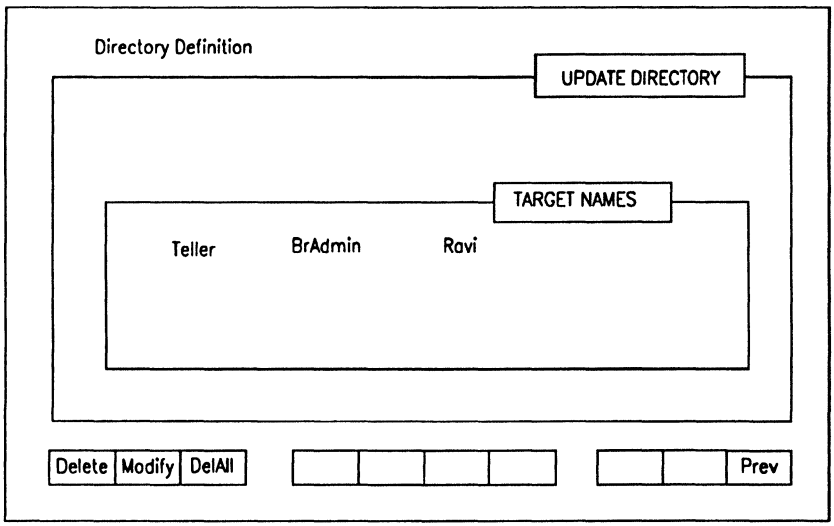
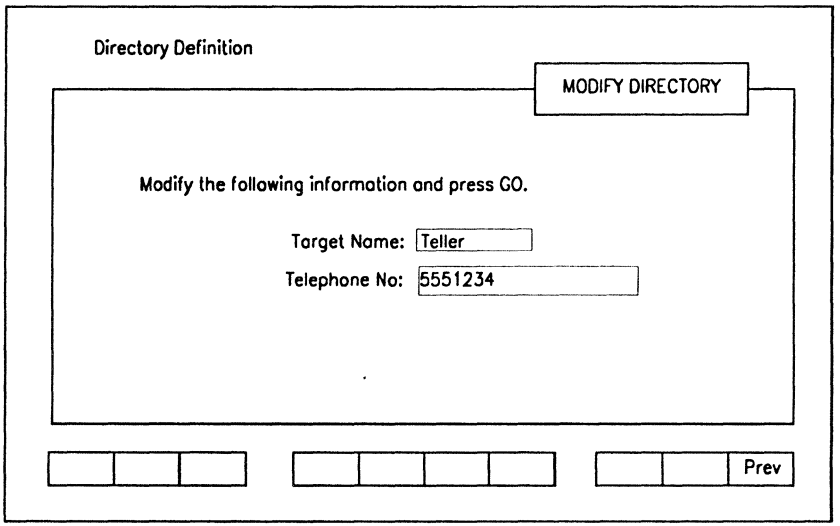


Figure 5-3. Modify Directory Screen



Using the Telephone Directory

Once you have created telephone entries, the Telephone Directory automatically provides telephone numbers and names to RAF RS-232 Source.

The telephone entries appear on the RAF RS-232 Source Dial-Up Menu. Refer to Section 7 for more information on loading and logging on to RAF RS-232 Source.

Exiting From the Telephone Directory

To exit from the Telephone Directory, use the following procedure:

1. To exit from the Telephone Directory, press **FINISH**.
2. Choose one of the following:
   - If you want to save the changes you made to the Telephone Directory, press **GO**.
   - If you do not want to save the changes you made to the Telephone Directory, press **FINISH** again.
   - If you want to continue working with the Telephone Directory, press **CANCEL**.

Section 6
Loading and Unloading RAF Services

This section explains how to load and unload RAF system services. It covers the following topics:

- RAF Loading Sequence
- Loading RAF Bridge
- Loading RAF Target
- Loading RAF RS-232 Target Interface Service
- Loading the Performance Gathering Service

Refer to Section 8 for information about loading the Message Posting services.

Before you can load the RAF system services and run RAF programs, you must complete the following tasks:

- Install RAF software on your system and network (Section 2)
- Create User Profiles for Source and Target workstations (Section 4)
- Create optional telephone directory entries (Section 5) and Script files (Section 4)

RAF Loading Sequence

Table 6-1 lists the correct sequence for loading RAF system services and related software. Your configuration may not require that you load all these services.

Table 6-1. RAF Loading Sequence

Order	Software Component	Location
1	Local Event Management (optional)	Any workstation
2	RAF Bridge	Target and Source server with Target cluster workstations
3	Mouse Service (optional)	Target and Source workstations to support mouse redirection
4	Device Service (optional; not required for EF 4552-DL2 MCR)	Target and Source workstations to support MCR redirection
5	MCR Service (optional)	Target and Source workstations to support MCR redirection
6	RAF Target	Target workstation or server
7	Modem Service	Target workstation or server using RS-232 Target Interface Service
8	RAF RS-232 Target Interface Service	Target workstation or server
9	Message Posting Bridge	Target and Source server with Target cluster workstations
10	Message Posting Service	Source and Target workstations
11	RAF PGS	Target workstation
12	Application Automator, Context Manager, CTOS Windows Services (all optional)	Any workstation

Note: *You cannot load RAF Target on an XE-520 or XE-530 server. You can load RAF RS-232 Target Interface Service on an XE-520 or XE-530 CP board with RS-232 ports. You cannot load it on any other processor board.*

If the BNet software you are using includes Modem Service, use that version; otherwise, use the Modem Service provided with RAF.

Refer to Section 8 for more information about the Message Posting Service.

Mouse Redirection

Mouse redirection is active only when a Source controls an entire Target workstation.

Only a character-mapped mouse cursor is supported; you cannot redirect mouse movements in graphical (bit-mapped) applications.

Note: *If you are using CTOS II 3.3, you must use version 3.3.3 or later.*

RAF Bridge

RAF Bridge runs on cluster servers that support Target cluster workstations. It receives RAF requests from RAF Source workstations and transports them to the Target workstations in the Cluster LAN. Multiple copies of RAF Source and RAF Target communicate through one RAF Bridge in a Cluster LAN. You do not need to load RAF Bridge if the cluster workstations have their own network connections.

Loading RAF Bridge

Use the following procedure to load RAF Bridge:

1. Type **RAF Load Bridge** on the Executive command line; then press **RETURN**.

   The following form displays:

```
RAF Load Bridge
  [Maximum Number of Targets and PGS (Default="5")]
  [Maximum Number of Concurrent Sessions (Default="3")]
```

   Refer to Table 6-2 for descriptions of the **RAF Load Bridge** parameters.

2. Fill in the parameters; then press **GO**.

Table 6-2. RAF Load Bridge Parameters

Parameter	Description
Maximum Number of Targets	Maximum number of Targets you expect to log on at one time Range: 1 to 128 Default: 5
Maximum Number of Concurrent Sessions	Maximum number of concurrent sessions between Source and Target workstations Range: 1 to 226 Default: 3

Note: *If the maximum specified number of concurrent sessions is reached, an additional Target user who attempts to log on receives an error message. The error message is recorded in the* Log.sys *file and reported to the Local Event Management, if installed.*

Unloading RAF Bridge

To remove RAF Bridge from memory, type **RAF Unload Bridge** on the Executive command line; then press **GO**.

RAF Target

You must load RAF Target on a Target workstation before a Source user can view or control that workstation. Any given Target workstation requires only one copy of RAF Target. You cannot load RAF Target on an XE-520 or XE-530.

Loading RAF Target

Use the following procedure to load RAF Target:

1. Type **RAF Load Target** on the Executive command line; then press **RETURN**.

   The following form displays:

```
RAF Load Target
    [Workstation ID(Default="RAF")]
    [Number of Sources(Default="1")]
    [Video Update Time Interval(Default="5")]
    [Notification(Default="no")]
    [Allow Viewing Only (Default="No")]
    [Allow MCR Redirection(Default="No")]
    [Allow ScrollFrame Redirection (Default="Y(es)")]
    [Allow Record & Playback (Default="Y(es)")]
    [Allow Printer Redirection (Default="N(o)")]
```

   Refer to Table 6-3 for information on RAF Load Target parameters.

2. Complete the command form as needed; then press **GO**.

Table 6-3. RAF Load Target Parameters

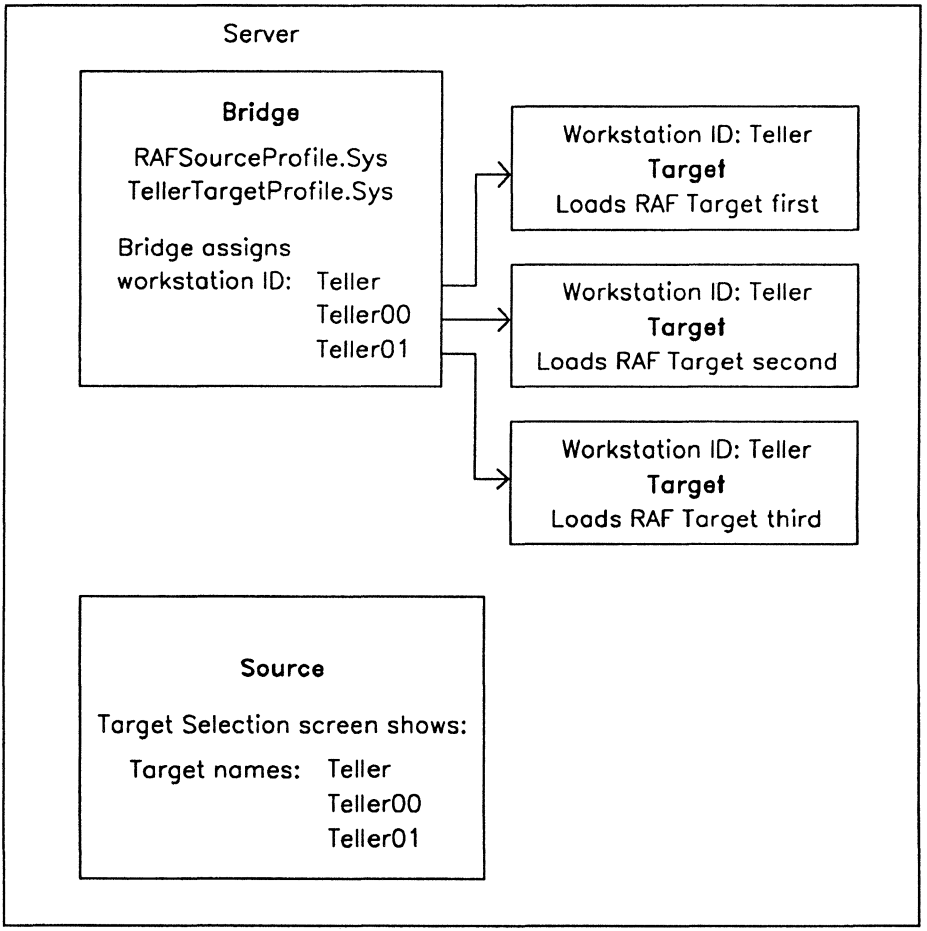
Parameter	Description
Workstation ID	ID of the Target Default: RAF If the ID you enter is in use, RAF assigns a unique ID by adding a two-digit suffix to the ID you enter. See Figure 6-1 for an example.
Number of Sources	Number of concurrent Source users who can view and/or control the Target Default: 1
Video Update Time Interval	Time interval in 1/10 seconds for updating the Source screen with the Target screen Range: 1 through 10 Default: 5
Notification	View or control session notification type Possible values: No No notification A Audio notification (beep) V Visual notification V indicates view session C indicates control session Default: No
Allow Viewing Only	Flag preventing control of Target Possible values: Yes Target can be viewed only No Target can be viewed and controlled Default: No

continued

Table 6-3. RAF Load Target Parameters (cont.)

Parameter	Description
Allow MCR Redirection	Flag allowing input from an MCR at the Source to be redirected to the Target Possible values: Yes RAF redirects MCR input to Target No RAF does not redirect MCR input Default: No ***Note:*** *If **Yes**, MCR Service must be installed at the Target and Source workstations. Device Service must be installed on the Target, except for the EF 4552-DL2 MCR, which requires MCR Service only.*
Allow ScrollFrame Redirection	Flag for controlling transmission of changed display lines to Source Possible values: Yes Transmit changed lines only No Transmit entire display Default: Yes **Yes** improves performance.
Allow Record & Playback	Flag allowing record and playback of Target activity Possible values: Yes Allow record and playback No Do not allow record and playback Default: Yes
Allow Printer Redirection	Flag allowing redirection of Target printer output to Source Possible values: Yes Allow printer redirection No Do not allow printer redirection Default: No

Figure 6-1. Duplicate Target ID Resolution



Unloading RAF Target

To remove the RAF Target Service from memory, type **RAF Unload Target** on the Executive command line; then press **GO**.

RAF RS-232 Target Interface Service

RAF RS-232 Target Interface Service provides an interface from the RAF Bridge and RAF Target to the RAF Source over RS-232 connections.

RAF RS-232 Target Interface Service supports only one Source-to-Target session at a time over a single RS-232 channel; however, each workstation can support up to six RS-232 channels by loading multiple copies of RAF RS-232 Target Interface Service. Each copy supports a unique specified channel.

When using RAF on a Modem Service network, you install the following system services:

- RAF Target on the Target workstation
- RAF RS-232 Target Interface Service on the Target workstation
- Modem Service on either the Target workstation containing RS-232 Target Interface Service or on the server in the Target's Cluster LAN. Refer to your Modem Service documentation for information about configuring and loading the Modem Service.

On an XE-520 or XE-530 processor, you can load RAF RS-232 Target Interface Service on a CP board with RS-232 connections. You cannot load it on any other processor board.

Loading RAF RS-232 Target Interface Service

Use the following procedure to load the RAF RS-232 Target Interface Service:

1. Type **RAF Load RS-232 Target Interface** on the Executive command line; then press **RETURN**.

   The following form displays:

```
RAF Load RS-232 Target Interface
   [Channel(Default="[comm]a")]
```

2. Enter the communications channel (serial port) connected to the modem; then press **GO**.

Unloading RAF RS-232 Target Interface Service

Use the following procedure to remove the RS-232 Target Interface Service from memory:

1. Type **RAF Unload RS-232 Target Interface** on the Executive command line; then press **RETURN**.

   The following form displays:

```
RAF Unload RS-232 Target Interface
   Channel Name
```

2. Enter the communications channel (serial port) serving the copy of the RAF RS-232 Target Interface Service you want to unload; then press **GO**.

Note: *You cannot unload RAF RS-232 Target Interface from memory on an XE-520 system. You must reboot the system using an initialization JCL file that does not load RAF RS-232 Target. To do so, you can use either of the following methods:*

- *Modify your standard JCL file and reboot.*
- *Use a JCL file associated with a different XE-520 key switch position. That JCL file should not include the RAF RS-232 Target Interface commands.*

Performance Gathering Service (PGS)

To monitor a Target's CPU activity, you use the performance gathering functions in RAF Source. You must therefore load the Performance Gathering Service before running the RAF Source program.

Loading PGS

Use the following procedure to load PGS:

1. **RAF Load PGS**, on the Executive command line; then press **RETURN**.

   The following form displays:

```
RAF Load PGS
   [Number of Sources (Default="1")]
```

2. To allow more than one Source at a time to monitor the Target's CPU, enter the number of Sources in the *[Number of Sources]* parameter; then press **GO**.

Unloading PGS

To unload PGS, type **RAF Unload PGS** on the Executive command line; then press **GO**.

Section 7
Managing a Distributed Environment With RAF

This section contains information on using RAF to manage workstations in a distributed environment. It covers the following topics:

- Using the online Help system
- Establishing connections with RAF Targets
- Monitoring
- Displaying CPU status
- Using printer redirection
- Changing the video update time interval
- Transferring files
- Recording and playing back sessions
- Using Chit-Chat

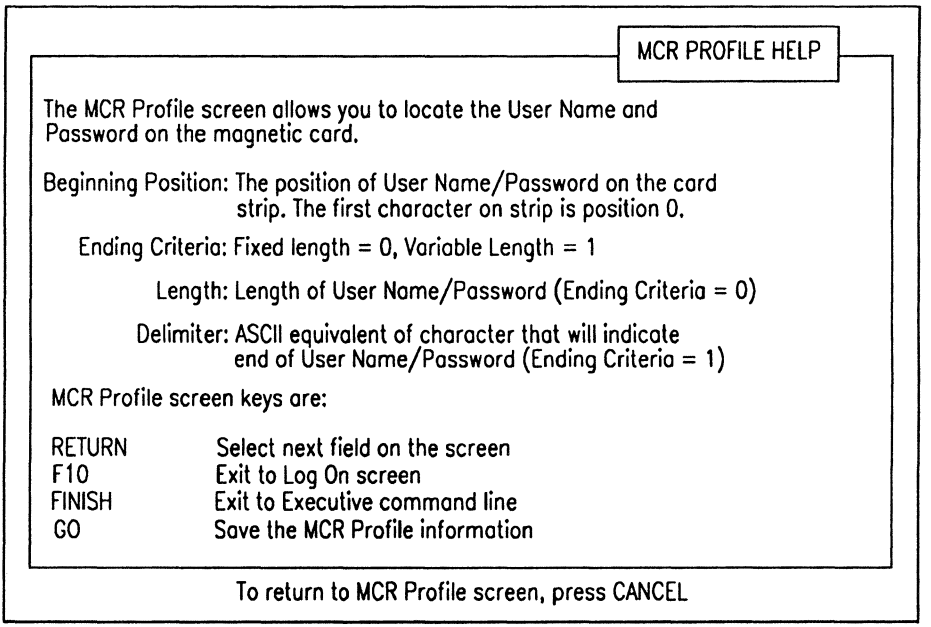
Using Online Help

RAF includes an online Help system that provides information about the current operation. You display the online Help by pressing the **HELP** key.

You can display a Help screen listing the **ACTION+KEY** combinations you use while monitoring a Target by pressing **ACTION+HELP**.

Figure 7-1 shows an example of a Help screen.

Figure 7-1. Example of a Help Screen


MCR PROFILE HELP
The MCR Profile screen allows you to locate the User Name and Password on the magnetic card.
Beginning Position: The position of User Name/Password on the card strip. The first character on strip is position 0.
Ending Criteria: Fixed length = 0, Variable Length = 1
Length: Length of User Name/Password (Ending Criteria = 0)
Delimiter: ASCII equivalent of character that will indicate end of User Name/Password (Ending Criteria = 1)
MCR Profile screen keys are:
RETURN Select next field on the screen
F10 Exit to Log On screen
FINISH Exit to Executive command line
GO Save the MCR Profile information
To return to MCR Profile screen, press CANCEL

Establishing Connections with RAF Targets

You use RAF Source to view or control a Target workstation or partition. There are two types of RAF Source programs:

- RAF Source
- RAF RS-232 Source

RAF Source runs on a Cluster LAN using CTOS Cluster Communications and on LANs and WANs using BNet II, and BNET.

RAF RS-232 Source runs on a Modem Service network for dial-up connections. The user interface is similar for both programs, except that RAF RS-232 Source provides a special menu for dial-up connections.

Table 7-1 shows the general process for establishing connections with a Target workstation. Once you have established a connection, you use the RAF Source features to view or control the workstation.

Table 7-1. Process for Establishing RAF Target Connections

Step Number	Step Name	Explanation
1	Start RAF Source	Run the RAF Source program from the CTOS Executive
2	Log on	Log on to RAF Source as a user
3	Select a Node	Select the node that contains the Target workstations you will access
4	Select a Target	Select a Target workstation at the selected node
5	Use RAF Source	Use RAF Source to monitor the Target and perform other functions

Establishing Connections with RAF Source

This subsection provides procedures for establishing Target connections with RAF Source. It covers the following topics:

- Starting RAF Source
- Logging onto RAF Source
- Selecting a Node
- Selecting a Target

Most of the steps for establishing connections with RAF Source and RAF RS-232 Source are the same. Figures 7-2 and 7-3 diagram both processes.

Figure 7-2. Establishing Connections with RAF Source

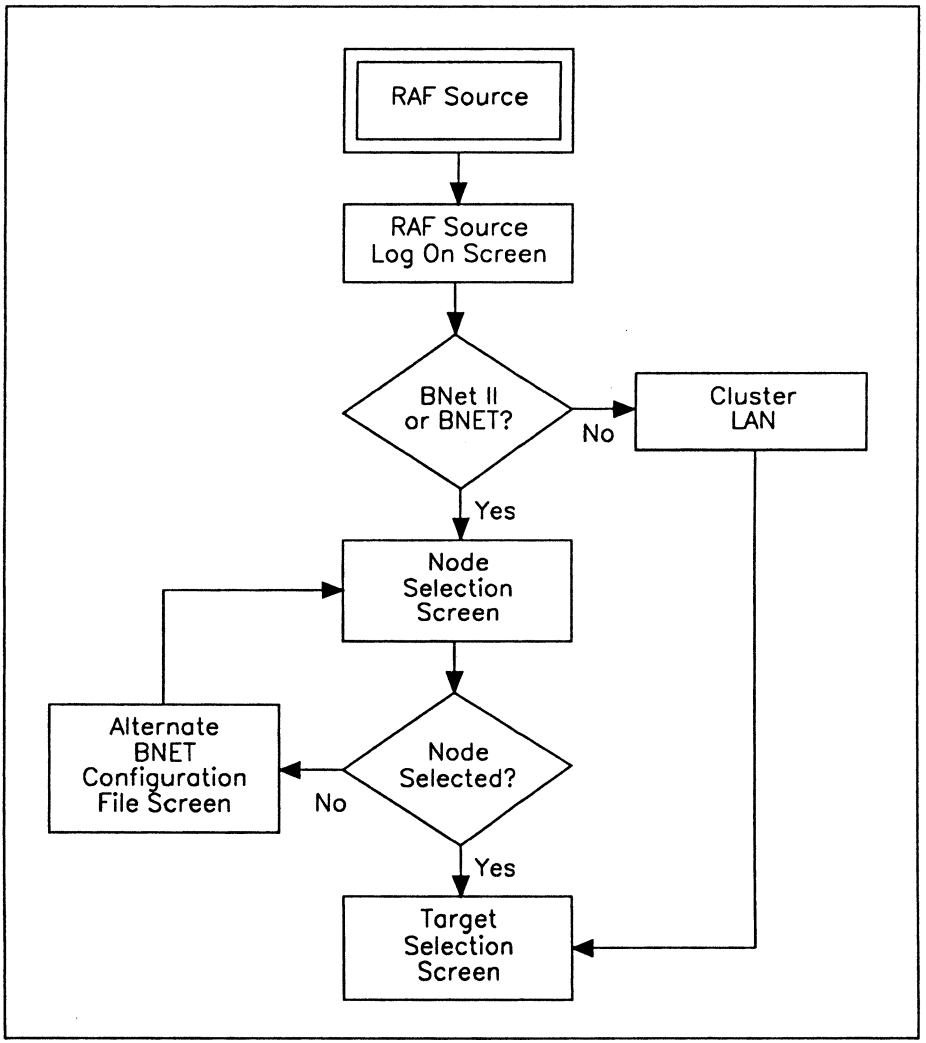
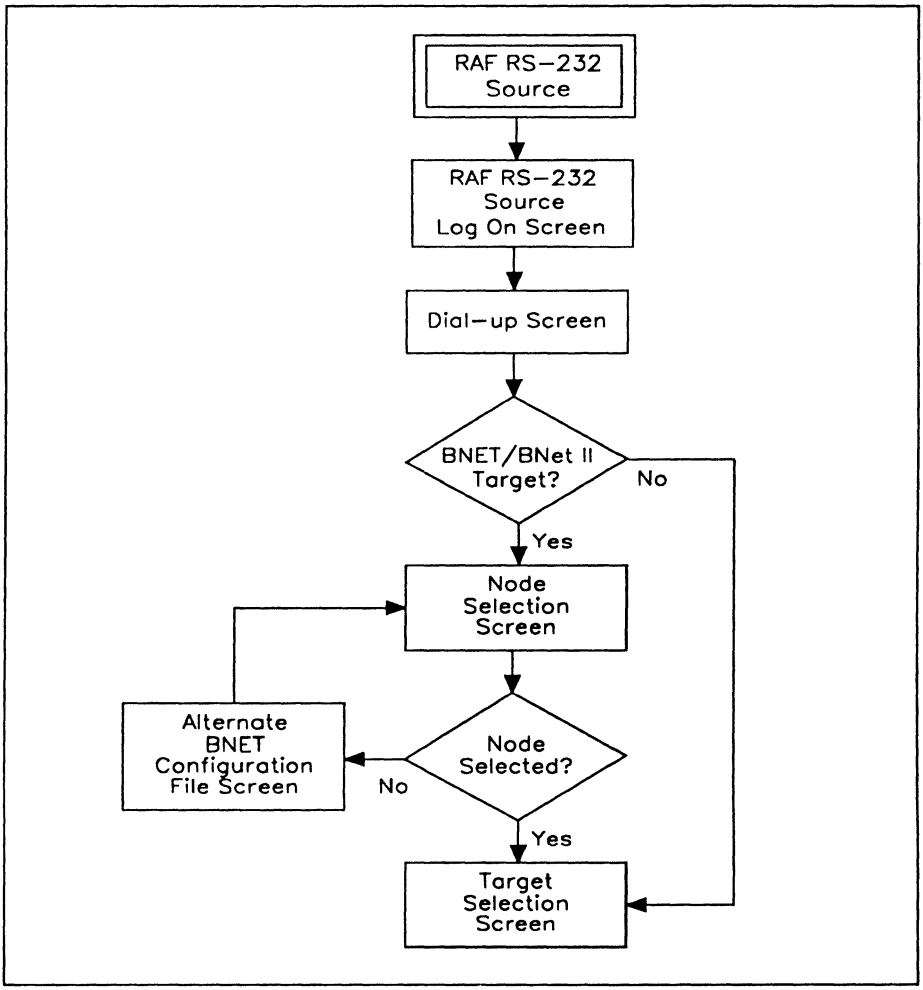


Figure 7-3. Establishing Connections with RAF RS-232 Source



Error Detection and Recovery

RAF RS-232 Source checks transmitted data for errors. If you have an error-correcting modem or are operating over communication lines that are not susceptible to data transmission errors, you can increase performance by switching off RAF RS-232's error checking. An E displaying in blinking reverse video in the top left corner of the screen indicates that error recovery is enabled; an N indicates that error recovery is not enabled.

If an error does occur when recovery is not enabled, Modem Service stops RAF and displays an error message.

Starting RAF Source and RAF RS-232 Source

Use the following procedure to start RAF Source or RAF RS-232 Source:

1. At the Executive command line, type **RAF Source** or **RAF RS-232 Source**; then press **RETURN**.

   The following form displays

```
RAF Source
 [Local Fonts (Default="Y(es)")]
 [Playback Filename (Default=None)]
 [ScriptFile (Default=None)]
 [TimeOut in min. (Default=30 min.)]
```

   Refer to Table 7-2 for information on RAF Source parameters.

2. Enter the parameter values; then press **GO**.

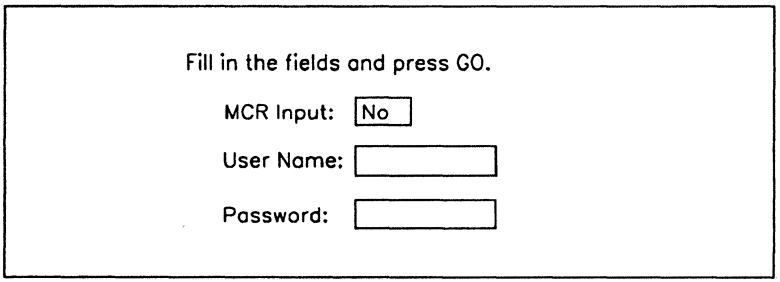
Table 7-2. RAF Source and RAF RS-232 Source Parameters

Parameter	Description
Local Fonts	Flag that determines which fonts RAF Source uses This is only available to workstations on a BNet II or BNET network. The parameter does not display on the RAF RS-232 Source Executive command form. Possible values: Yes RAF uses the fonts available on your workstation No RAF uses fonts from the Target workstation Default: Yes
Playback Filename	Name of a playback file recorded by the RAF recording utility To replay a file of recorded Target activity, enter the file name. You cannot access other RAF features while playing back a file.
ScriptFile	Name of a script file you have created for automating access to a Target Refer to Section 4 for more information about script files.
TimeOut	The number of minutes that may elapse without Source activity before RAF automatically terminates the session Range: 1 to 180 Default: 30

Logging On to RAF Source and RAF RS-232 Source

After you start RAF Source, the RAF Log On menu shown in Figure 7-4 displays.

Figure 7-4. RAF Source Log On Menu



This menu is the same for RAF Source and RAF RS-232 Source. If you are using an MCR device other than an EF 4552-DL2 , you must install Device Service before you can log on using the MCR device, and the MCR device must be identified as **MCR1** in the device configuration file.

Fill in the requested information; then press **GO**. If you enter **Yes** for *MCR Input*, RAF prompts you to swipe your MCR card for the user name and password.

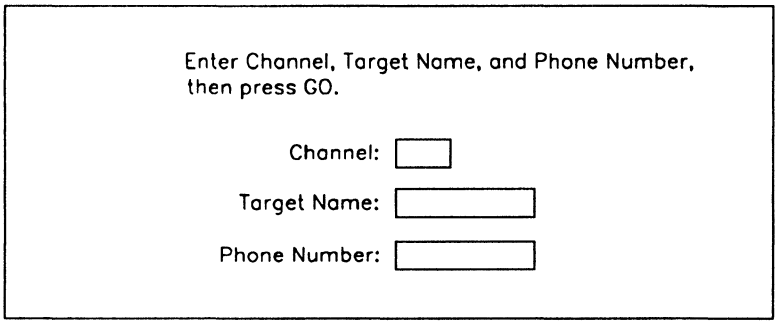
The following table shows which subsection to refer to depending on your configuration.

Configuration	Subsection
RAF just within a cluster LAN	Selecting a Target
RAF over BNET or BNet II	Selecting a Node
RAF RS-232 Source	Using the Dial-up Menu

Using the Dial-Up Menu

The following dial-up menu displays after you log onto RAF RS-232 Source.

Figure 7-5. Dial-Up Menu Screen



If a phone directory exists, the Telephone Directory entry and phone number display as defaults.

Use the following procedure to complete the dial-up menu:

1. Enter the channel name.

   Refer to Appendix C for channel name examples.

2. Choose one of the following:

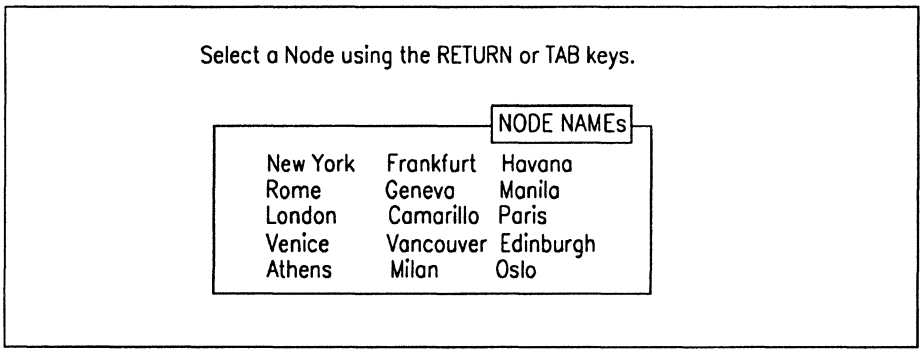
   - If no phone directory exists, enter the Target name and phone number.
   - If you are using the phone directory, enter the Target name and step through the phone directory.

3. Press **GO**.

Selecting a Node

After you have logged on to RAF or, for RAF RS-232 Source only, established communications with a system that has BNet loaded, the Node Selection menu shown in Figure 7-6 displays.

Figure 7-6. RS-232 Node Selection Menu



If the Source workstation is a BNet cluster node, its server's node name displays first in the list of node names. If the Source workstation is connected to an Ethernet LAN, its own node name also displays.

To display the Targets available on a node, move the cursor to the node name you want to access; then press **Target (F2)**.

Table 7-3 lists the Node Selection menu options.

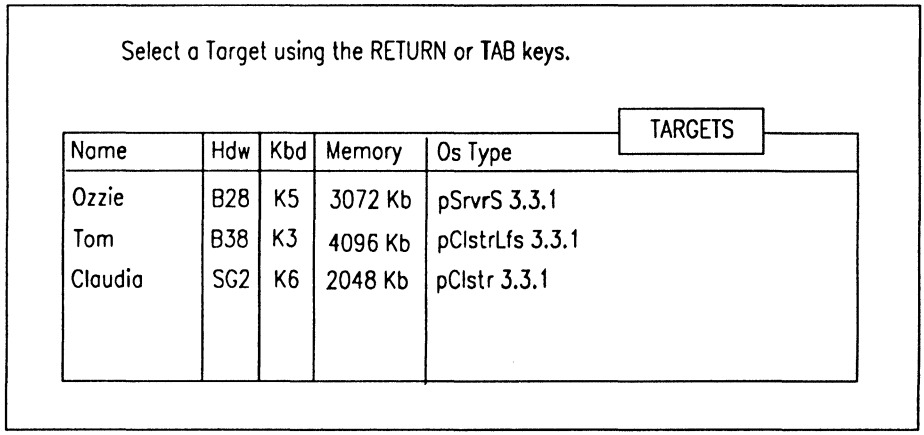
Table 7-3. Node Selection Menu Options

Key	Function
F1	Update the Target Node Selection screen
F2	Display the list of Target workstations at the highlighted node
F3	Display a list of nodes contained in a different classic BNET configuration file
F9	Manually enter a node name
F10	Return to the Log On screen

Selecting a Target

Once you have selected a node and pressed the **Target (F2)** key, the next screen displays a list of Target workstations, as shown in Figure 7-7.

Figure 7-7. Target Selection Screen



Select a Target with the **RETURN** or **TAB** key. RAF highlights your selection. Then use the function keys to select a task. Table 7-4 explains the functions of the keys.

Table 7-4. Target Selection Function Keys

Key	Function
F1	Update the Target selection list.
F2	Transfer a file to or from an RS-232 Target.
	Refer to Transferring Files for more information.
F3	Select a partition on the highlighted Target.
	Refer to Selecting a Partition for more information.
F4	Display a Target's screen on the Source screen.
	Refer to View Mode for more information.
F5	Allow the Source user to perform operations on the Target workstation while locking out the Target keyboard.
	Refer to Control Mode for more information.
SHIFT+F5	Allow the Source user to enter the CTOS Debugger on the Target.
	Refer to Remote Debugging for more information.
F6	Examine in succession each Target on the node or each partition on a Target.
	Refer to Scan Mode for more information.
F7	Display CPU activity of the Target workstation.
	Refer to Displaying CPU Status for more information.
F8	Toggle printer redirection on and off.
	Refer to Using Printer Redirection for more information.
F9	Change the video update time interval.
	Refer to Changing the Video Update Time Interval for more information.
F10	Return to the Node Selection screen.

Selecting a Partition

Use the following procedure to select a partition on a Target workstation:

1. Highlight a Target workstation on the Target Selection screen by using the **RETURN** or **TAB** keys; then press **F3**.

   A list of application partitions on the Target workstation displays; system service partitions do not display.

2. Highlight a partition by using the **RETURN** or **TAB** keys.
3. Select one of the function keys shown in Table 7-5.

Table 7-5. Partition Selection Function Keys

Key	Function
F1	Update the list of partitions.
F2	Transfer a file to or from a RAF RS-232 Target.
F4	View the selected partition.
F5	Start a control session with the selected partition.
F6	Examine in succession snapshots of each partition on the Target workstation. Refer to Scan Mode for more information.
F7	Display CPU activity of the Target workstation. Refer to Displaying CPU Status for more information.
F8	Toggle printer redirection on and off. Refer to Using Printer Redirection for more information.
F10	Return to the Target Selection screen.

Monitoring Workstations

RAF allows you to monitor a workstation in four modes:

- View
- Control
- Scan
- Remote Debugging

The specifications in the RAF Target user profile determine the modes available on a given Target to a given user. Table 7-6 lists the monitoring modes and describes each.

Table 7-6. Monitoring Modes

Mode	Description
View	Displays a Target's screen on the Source's screen. You see the operations performed by the Target user.
Control	Allows the Source user to perform operations on the Target workstation while locking out the Target keyboard, except for Action keys.
Scan	Allows you to take a snapshot of the current screen of each Target workstation in a Cluster LAN or each partition of a single Target workstation.
Remote Debugging	Functions similar to Control mode, but allows users to enter the debugger and debug applications.

View Mode

You access the View mode at the Target Selection Screen or Partition Selection Screen. View mode shows the Target screen and periodically updates it on the Source user's screen. The Target user can continue working because the keyboard is not disabled. Conversely, the Source user cannot send keystrokes to the Target.

To access View mode, press **View (F4)** at the Target or Partition Selection screen. The following message displays:

```
Initializing Session, Please Wait. . .
```

When the Session starts, the Target's screen displays on the Source's screen.

If the notification option is on, RAF tells the Target user that the workstation is being viewed or controlled. The notification options include an audible beep or a visual notification, which is a single character displayed at the top of the screen. A `V` indicates a View session, and a `C` indicates a Control session.

If there are fewer lines or columns on the RAF Source workstation than on the RAF Target workstation that is being viewed, the display shows as many lines and columns as possible, starting at line 0 and column 0. Use the **ACTION** keys to change the starting line and column.

Action Keys for View Mode

Table 7-7 lists key sequences available to the Source user during a View session.

Table 7-7. Action Keys for View Mode - Source

Keys	Description
ACTION+RightArrow	Shift display right one column
ACTION+LeftArrow	Shift display left one column
ACTION+UpArrow	Scroll up one line
ACTION+DownArrow	Scroll down one line
ACTION+PrevPage	Display top lines of the Target
ACTION+NextPage	Display bottommost lines of the Target
ACTION+T	Start or stop a Chit-Chat session with the Target
ACTION+W	Display the name of the currently monitored Target
ACTION+L	Display leftmost columns
ACTION+R	Display rightmost columns
ACTION+E	Enable or disable error recovery mode (RAF RS-232 Source only)
ACTION+Q	Query current error recovery mode (RAF RS-232 Source only)
ACTION+Help	Displays the Help screen for RAF Action Keys
ACTION+Cancel	Return to the Target or Partition Selection screen
ACTION+X	Exit from RAF and return to the Executive command line

Control Mode

In Control mode, a Source workstation controls a Target workstation or partition. Video from the Target workstation or partition displays on the Source workstation. Keystrokes typed at the Source workstation are sent to the Target, which processes them as if they were typed on the Target workstation keyboard. If the RAF Source and Target keyboards are different, RAF beeps and ignores keystrokes on the Source that have no equivalent on the Target. A Target workstation can be controlled only if that Target was installed with the *[Allow viewing only]* parameter set to **No**.

When a Source workstation controls an entire Target workstation, the local keyboard is unavailable to the Target user. When a Source workstation controls a Target partition, installing Context Manager in Target memory allows local keyboard use in any partition other than the controlled partition.

During a control session, holding a key down does not cause it to auto-repeat. RAF Source discards auto-repeat signals because various CTOS applications interpret key-down conditions differently. You must press and release the appropriate key for each character you require.

Starting a Control Session

To begin a control session, press **Control (F5)** on the Target or Partition Selection screen. The following message displays:

```
Initializing Session, Please Wait. . .
```

The Target's screen displays on the Source's screen.

If the notification option is on at the Target workstation, a visual or audible indicator notifies the Target user that the workstation is being monitored. Notification may not be visible during control of a background partition until that partition is brought to the foreground.

Note: *A Source user controlling a background partition on a Target cannot send Context Manager* **ACTION+KEY** *keystrokes for changing the current partition.*

Action Keys for Control Mode

You can use the action keys listed in Table 7-8 to manipulate the display of the Target screen during a control session.

Table 7-8. Action Keys for Control Mode

Action Keys	Description
ACTION+RightArrow	Shift display right one column
ACTION+LeftArrow	Shift display left one column
ACTION+UpArrow	Scroll up one line
ACTION+DownArrow	Scroll down one line
ACTION+PrevPage	Display top lines of the Target
ACTION+NextPage	Display top lines of the Target
ACTION+T	Start or stop a Chit Chat session with a Target
ACTION+R	Display rightmost columns
ACTION+L	Display leftmost columns
ACTION+W	Display name of currently monitored Target
ACTION+'	The key pressed after this combination is sent as an Action Key in control mode only.
ACTION+E	Enable or disable error recovery mode (RAF RS-232 Source only)
ACTION+Q	Query current error recovery mode (RAF RS-232 Source only)
ACTION+'N	Enable or disable monitoring notification

continued

Table 7-8. Action Keys for Control Mode (cont.)

Action Keys	Description
ACTION+K	Toggle between interactive and block transmission modes. Control sessions begin in interactive mode. A `B` or an `I` displays in the upper-left corner of the screen to indicate whether you are in block or interactive mode.
ACTION+Cancel	Return to the Target or Partition selection screen
ACTION+X	Exit from RAF
ACTION+Help	Display the Help screen for RAF Action Keys

Remote Debugging

A remote debugging session allows a Source user to perform debugging on the Target. A remote debugging session is the same as a control session except that the CTOS Debugger is available to the Source user. This feature is accessible only to privileged users. Remote debugging is available only to a user controlling the entire workstation, when no other RAF sessions are in progress with that workstation.

During a remote debugging session, the Target user can also use the keyboard.

Starting a Remote Debugging Session

To start a remote debugging session, press **SHIFT+F5** on the Target selection screen. In addition to the normal control session keys, the keys listed in Table 7-9 are also available. If the Debugger is not installed on the Target workstation, RAF ignores these remote debugging Action keys.

Table 7-9. Action Keys for Remote Debugging

Action Keys	Description
ACTION+'A	Start or stop a single-process debugging session
ACTION+'B	Start or stop a multi-process debugging session

Scan Mode

In Scan mode, RAF displays a snapshot of the current screen of every Target in a cluster LAN, one at a time. It can also display snapshots of each partition on a Target. Beginning with the first selected Target or partition, you can look at the current screen and then move to the current screens of other Targets or partitions in succession. You cannot scan your own workstation.

Scan mode differs from View mode or Control mode because it shows a static display of a single current screen or partition. It does not show additional screen changes that may take place on the Target, nor can you control the Target's keyboard. Scan is useful for taking a quick look at the entire network to determine which workstation you wish to view or control.

You press **ACTION+RETURN** to move through the current screens of the Target workstations, or the partitions on a single Target. When you reach the screen of the last workstation or partition, the display returns to the first screen that you scanned.

Starting a Scan Mode Session

To enter Scan mode, press **Scan (F6)** at the Target Selection Screen or Partition Selection Screen.

A message displays:

```
Initializing Session, Please Wait. . .
```

When the Session starts, the Target's screen displays on the Source screen.

If the notification option is on at the Target, visual or audible indicator notifies the Target user of monitoring by a Source; however, notification may not be visible during a scan session of an inactive partition.

Action Keys for Scan Mode

You can manipulate the display of the Target screen during a Scan session by using Action or function keys, return to a previous screen, or exit from RAF.

Table 7-10 shows the action key sequences available to the Source user during a Scan session.

Table 7-10. Action Keys for Scan Mode

Action Keys	Description
ACTION+RightArrow	Shift display right one column
ACTION+LeftArrow	Shift display left one column
ACTION+UpArrow	Scroll up one line
ACTION+DownArrow	Scroll down one line
ACTION+PrevPage	Display top lines of the Target
ACTION+NextPage	Display bottommost lines of the Target
ACTION+L	Display leftmost columns
ACTION+R	Display rightmost columns
ACTION+Return	Move to next Target or partition screen
ACTION+1	Update the current screen
ACTION+Cancel	Return to the Target or partition selection screen
ACTION+X	Exit from RAF

Displaying CPU Status

You can monitor a Target's CPU activity by using the Interactive Performance Monitor (IPM). The IPM displays information about the Target's CPU utilization, collected by the Performance Gathering Service (PGS). It uses the display shown in Figure 7-8. PGS must be loaded on the Target workstation. The IPM is useful for determining the load on the Target workstation's CPU.

IPM displays performance on a percentage scale. The bar graph indicates the percentage of time that the processor is busy. The bars are incremented in units of 5 percent. As CPU activity increases, the bars become fainter near the top.

For information on loading PGS, refer to Section 6.

Figure 7-8. Interactive Performance Monitor Screen

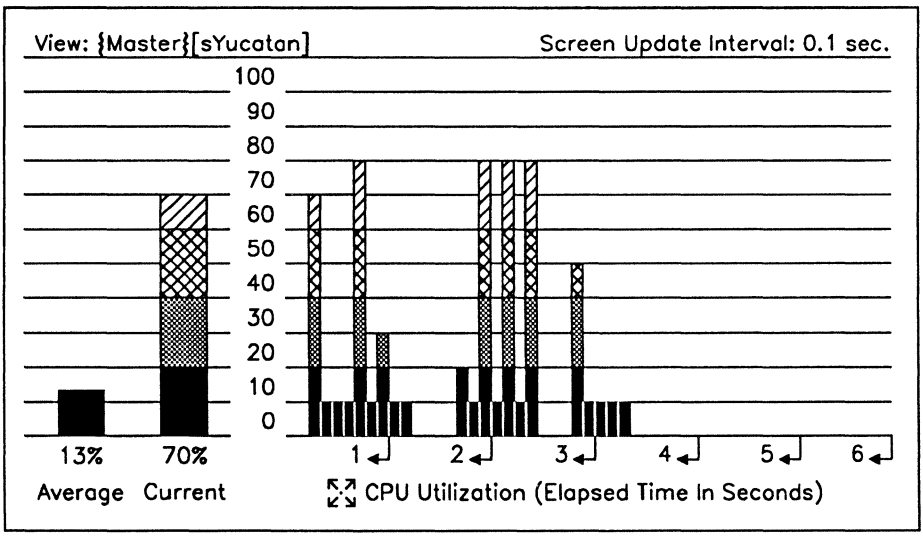


Table 7-11. Elements of the Interactive Performance Monitor Display

IPM Display Element	Description
View indicator	The target workstation you are viewing
Update interval	The duration in seconds of the sampling period
	During this period, IPM samples the activity every 0.01 seconds then displays the average of those samples at the end of the period.
	Range: 0.1 to 12.5 seconds
Average	The average of all the CPU activity samples, both current and elapsed, displayed on the screen
Current	The average amount of CPU activity during the last sampling period
Elapsed	A history of the Current values
	The leftmost bar is the same as the Current value

For example, if you set the update interval to 0.1 seconds, the PGS accumulates 10 samples and IPM displays the average of those 10 samples as the current CPU utilization. After the next 0.1-second interval, IPM displays the new current average, the new and previous current averages in the elapsed section, and the average of all the averages.

Starting the Interactive Performance Monitor

To start IPM, press **Status (F7)** at a Target or Partition Selection Screen.

Keys for the Interactive Performance Monitor

Table 7-12 describes the keystrokes available in the IPM.

Table 7-12. Keys for the Interactive Performance Monitor

Keys	Description
F4	Increase update interval by one second
F5	Increase update interval by one tenth second
F6	Decrease update interval by one second
F7	Decrease update interval by one tenth second
ACTION+Cancel	Exit from the IPM screen

RAF Target Action Keys

Table 7-13 lists the Action key combinations available to a user at a RAF Target workstation.

Table 7-13. Action Keys for View Mode - Target

Keys	Description
ACTION+F	Find monitoring Source user(s)
ACTION+M	Enable or disable Source monitoring
ACTION+N	Enable or disable monitoring notification The *[Notification]* option in the **RAF Load Target** command must be **Yes** for this option to work.
ACTION+T	Start or stop a Chit-Chat session

Redirecting Printer Output

You can redirect printer output from the Target workstation to the Source workstation. When printer redirection is on, the **PrnRdx (F8)** key is highlighted.

You press the **PrnRdx (F8)** key to turn redirection on and off.

For printer redirection to work, the following conditions must be met:

- Queue Manager must be installed on the Target and Source workstations. Queue Manager is supplied with both Standard Software and GPS.
- The *Queue.index* file or GPS queue specification must be the same at the Target and Source.
- When RAF Target is loaded, the parameter for printer redirection must be set to **Yes**.

Changing the Video Update Time Interval

When you view or control a Target workstation, your screen is updated at intervals of 500 milliseconds. You can change the Video Update Time Interval to increase or decrease the time interval. If the interval is too small, RAF Target sends video updates too frequently, which degrades Target performance.

Use the following procedure to change the Video Update Time Interval:

1. At the Target Selection Screen, press **Change (F9)**.
2. Enter a new time interval; then press **Prev (F10)**.

Recording and Playing Back Sessions

You can record a RAF session with a Target and replay it later. RAF provides Executive commands for starting and stopping the recorder. You use RAF Source or RAF RS-232 Source to play a recording back.

Starting a Recording Session

Use the following procedure to record a session:

1. To start a recording, type **RAF Start Screen Recording** on the Executive command line; then press **RETURN**.

   The following form displays. Table 7-14 describes each parameter.

```
RAF Start Screen Recording
    Record file name
    [NodeName = (Default = Local Node)]
    [WorkStation Name = (Default = Local Target)]
    [Partition Name = (Default = Primary)]
```

2. Complete the command form; then Press **GO**.

After recording starts, you can view, control, or scan the Target being recorded or monitor another Target. If you monitor another Target, RAF does not record that Target's activity. Screen recording of the primary partition continues until you stop the recording session.

Note: *If the Target screen changes frequently, the screen recording file grows rapidly. Ensure that a long recording session does not use all your available disk space.*

Table 7-14. RAF Start Screen Recording Parameters

Parameter	Description
Record file name	The name for a file containing the recorded session
NodeName	The name of the node to which the Target is connected
Workstation Name	The name of the Target workstation
Partition Name	The name of the partition you want to view and record

Naming the Record File

For best performance, if you are recording a Target on another node, specify a record file on that node.

RAF at the Target workstation interprets the record file name as though you had entered it at the Target; therefore, for example, *[!Sys]* is the system volume on the Target server, not the Source server.

Note: *You play the file back with RAF Source, which interprets the file name at the Source workstation; therefore, the file name you specify for recording must be accessible from the Source workstation.*

Table 7-15 provides some examples of recording file names based on the configuration in Figure 7-9.

Table 7-15 assumes that workstations with local storage boot from their local hard disk. All workstations except T4 have local storage. The current path on all workstations is *[Sys]<Sys>*.

Figure 7-9. RAF Recording Sample Configuration

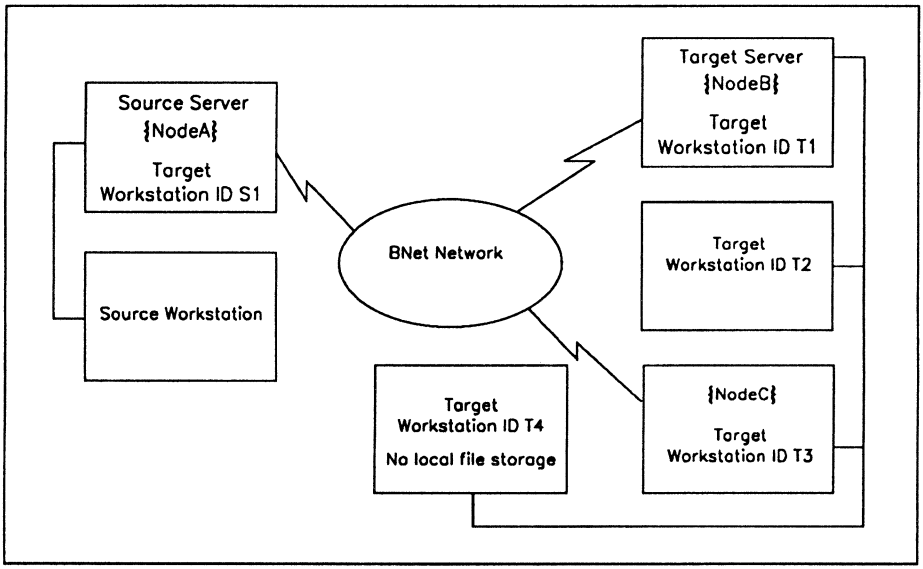


Table 7-15. RAF Recording File Name Examples

Target ID	Record File Name Specification	Record File Physical Location	Playback File Specification at Source
S1	[Sys]<Sys>FileA	S1	[!Sys]<Sys>FileA
T2	[Sys]<Sys>FileA	T2	Not available from Source
T2	[!Sys]<Sys>FileA	T1	{NodeB}[Sys]<Sys>FileA
T2	{Local}[Sys]<Sys>FileA	T2	Not available from Source
T2	{NodeA}[Sys]<Sys>FileA	S1	[!Sys]<Sys>FileA
T3	[Sys]<Sys>FileA	T3	{NodeC}[Sys]<sys>FileA
T3	[!Sys]<Sys>FileA	T1	{NodeB}[Sys]<Sys>FileA
T4	[Sys]<Sys>FileA	T1	{NodeB}[Sys]<Sys>FileA

Stopping a Recording Session

Use the following procedure to stop a recording session:

1. Type **RAF Stop Screen Recording** on the Executive command line; then press **RETURN**:

   The following form displays:

```
RAF Stop Screen Recording
   [NodeName = (Default = Local Node)]
   [WorkStation Name = (Default = Local Target)]
```

2. Enter the node and Target names, if necessary; then press **GO**.

If you entered the node name or workstation name when starting the recording, you must also enter them here.

The recording file contains the Target activity, which you can now play back.

Playing Back a Recorded Session

Use the following procedure to play back a recording of a RAF session:

1. Type **RAF Source** or **RAF RS-232 Source** on the Executive command line; then press **RETURN**.

   The following form displays:

```
RAF Source
   [Local Fonts(Default="Y(es)"]
   [Playback Filename (Default = None)]
   [ScriptFile (Default = None)]
   [Timeout in min. (Default = 30min.)]
```

2. Enter the name of the recording file in the *Playback Filename* field; then press **GO**.

   The RAF Source program starts and the Log On Screen displays.

3. Enter your user name and password; then press **GO**.

RAF Source replays the script file. At the beginning and end of the playback and while the playback is paused, the Playback Help Bar shown in Figure 7-10 displays at the top of the screen. The caret (^) represents the **CODE** key. The functions on the help bar are similar to those on a videotape player. To move through a playback session, select an option from the bottom row by pressing the appropriate keys in the top row. Table 7-16 describes the actions of each key.

The RAF Source parameters other than *[Playback Filename]* are the same as when you are not using the playback feature. Enter as much of the playback file path as necessary to clearly identify the file from the Source workstation. Refer to Figure 7-9 and Table 7-15 for some examples of recording file names and how you access the recording files as playback files.

Figure 7-10. Playback Help Bar

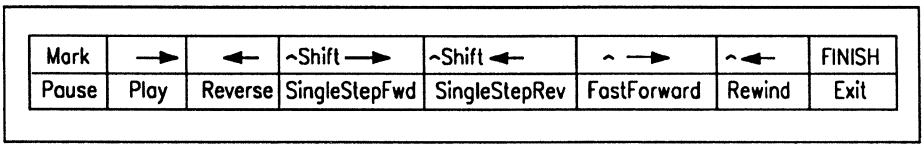


Table 7-16. Playback Keys

Function	Key Strokes	Description
Pause	MARK	Pauses the playback
Play	RightArrow	Plays the session forward
Reverse	LeftArrow	Plays the session backward
Single Step Forward	CODE+SHIFT+RightArrow	Plays the session forward one screen and a time
Single Step Reverse	CODE+SHIFT+LeftArrow	Plays the session backward one screen and a time
Fast Forward	CODE+RightArrow	Advances the recording at high speed
Rewind	CODE+LeftArrow	Rewinds the recording at high speed
Exit	FINISH	Exits from playback and returns to the Executive command line
Help	HELP	Displays the help bar while the recording is playing back

Transferring Files

RAF allows you to transfer files over a Modem Service network using the RAF RS-232 Source program. You can transfer files to or from a Target node that is accessible by the RAF RS-232 Target Interface Service. Disabling a Target does not affect a file transfer that is in progress.

Use the following procedure to transfer files between the Source and the Target:

1. At the Target Selection Screen, press **FileXr (F2)**.

   The File Transfer Menu displays.

2. Choose one of the following:

   - To transfer a file from the Source to the Target, press **SendTo (F1)**.
   - To transfer a file from the Target to the Source, press **RcvFrom (F2)**.

3. Enter the name of the file you are transferring in the *From Filename* field.
4. Enter the name you want to assign to the transferred file in the *To Filename* field.
5. Enter **Binary** in the *Transfer Format* field to transfer all file types; then press **GO**.

If the file exists at the destination, the following message displays in the File Transfer Menu:

```
Status: Dest Exists: Press GO to Overwrite, CANCEL to Deny.
```

To terminate a file transfer session, press **ACTION+CANCEL**. The following message displays:

```
File Transfer Aborted
```

Using Chit-Chat

The Chit-Chat feature allows Source and Target users to communicate through dialog windows during a monitoring session. Either a Source or Target user can initiate a Chit-Chat session during a View or Control session. Chit-Chat is useful for troubleshooting installation or programming concerns and for communicating interactively with a remote user. Chit-Chat does not allow you to save interactive messages, but allows you to communicate quickly as the need arises.

You cannot use Chit-Chat in the following circumstances:

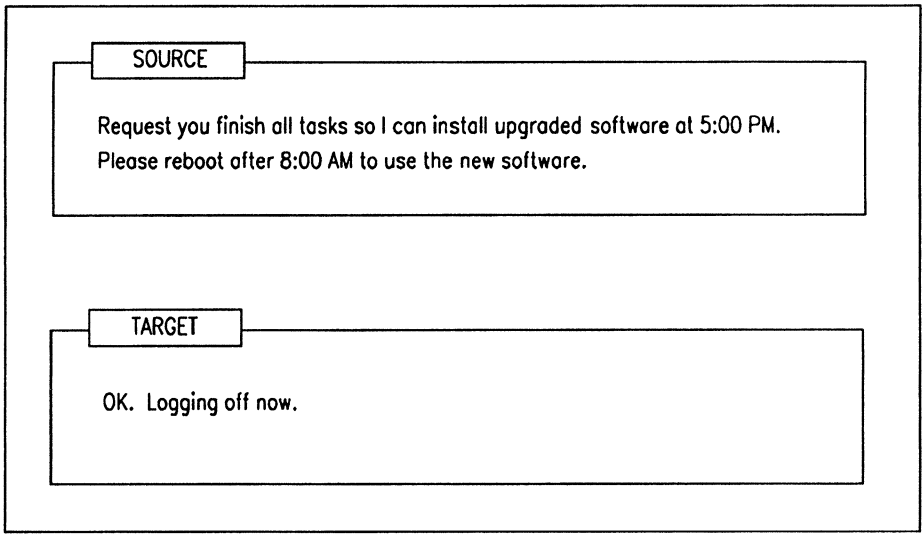
- The Target workstation is in the debugger
- You are in a remote debugging session
- You are not in a View/Control session

Additionally, the application running on the Target must be an interactive one waiting for a keystroke.

To use Chit-Chat press **ACTION+T** during a monitoring session. The dialog windows shown in Figure 7-11 display on both the Source and Target. Any information that the Source or Target users type, displays in the appropriate dialog window at both workstations. The text in the windows scrolls as you type.

Use **ACTION+T** to end the Chit-Chat session.

Figure 7-11. Chit-Chat Screen


SOURCE
Request you finish all tasks so I can install upgraded software at 5:00 PM.
Please reboot after 8:00 AM to use the new software.
TARGET
OK. Logging off now.

Section 8
Sending Messages to Other RAF Users

This section provides information on RAF Message Posting, including information on:

- Message Posting components
- loading the Message Posting services
- creating messages
- saving and recalling messages
- sending messages
- creating and modifying distribution lists
- displaying received messages and acknowledgements

About Message Posting

Message Posting is a useful notification system for quickly distributing important messages to users on a network.

You can use Message Posting to send a broadcast message to:

- a user on another workstation
- users on several workstations
- users on other BNet nodes

Messages can be up to four lines long with 50 characters per line. You can store up to 10 messages you have created and send them later. You can address messages using either node names or user names.

You can use Message Posting on a Cluster LAN, BNet II, or BNET network. Figure 8-1 shows Message Posting on a Cluster LAN; while Figure 8-2 shows Message Posting on a BNet II network.

Figure 8-1. Message Posting on a Cluster LAN

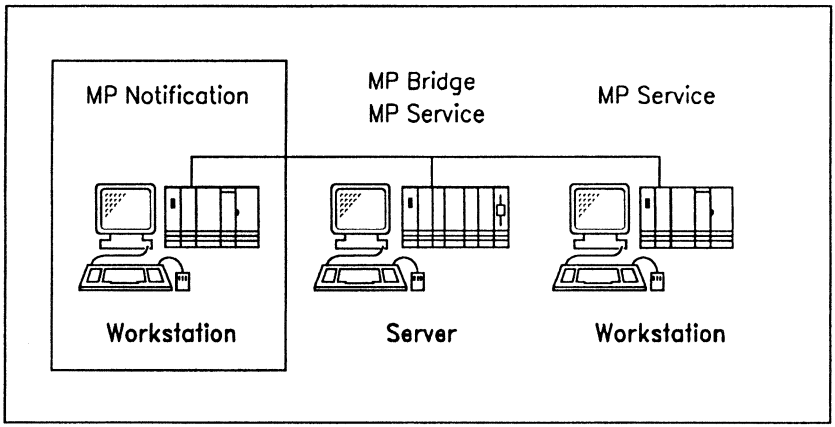
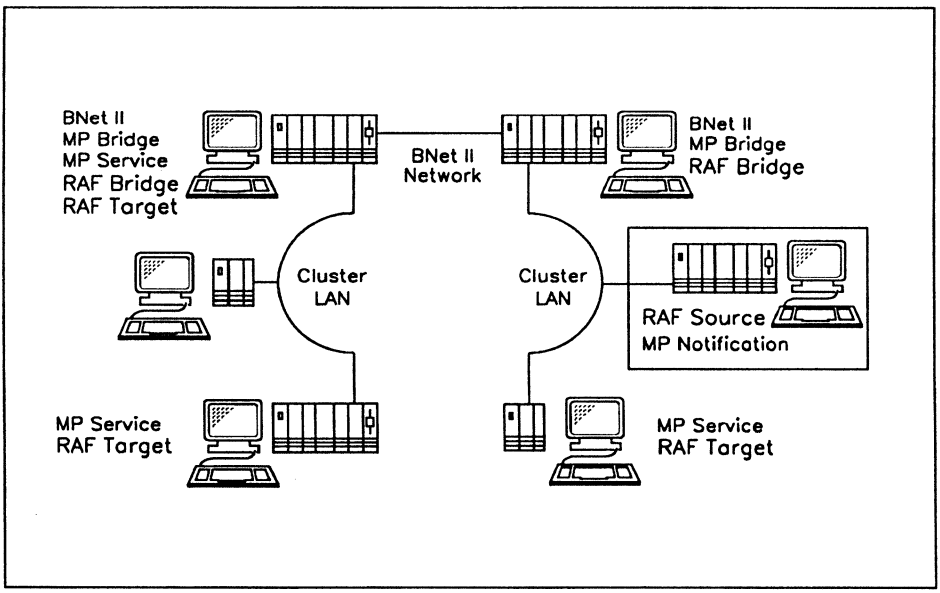


Figure 8-2. Message Posting on a BNet II Network



If the Message Posting Bridge is loaded in memory at the the server, you can use Message Posting Notification at any workstation on the cluster. You should load the Message Posting Service in memory on any workstation that receives messages.

Note: *You can load the Message Posting Bridge component only in memory on an XE. You cannot load other Message Posting components.*

If you receive the error message, `Unable to access the node`, this may indicate that you did not install the Message Posting Service on the remote node, rather than indicate a communication error. Refer to section 2 for installation instructions.

Note: *To send messages over BNet, you should install BNet with the* `Large Request Buffer` *parameter (BNet II 2.1) or* `Max Request Size` *parameter (BNet II 3.0) set to 2612 or greater. A smaller value can result in an* `Unable to access the node` *error message.*

Message Posting Components

Message Posting contains three components, as shown in Table 8-1.

Table 8-1. Message Posting Components

Component	Description	Location
Message Posting Notification	The user interface to create, send, retrieve, or store messages.	Source and Target workstations
Message Posting Service	The system service that receives messages at the destination.	Source and Target workstations
Message Posting Bridge	The system service that transports messages in a Cluster LAN.	Server in each Cluster LAN

Loading Message Posting

Load the Message Posting services and program in the order shown in Table 8-2. Load and unload Message Posting Bridge and Message Posting Service with the commands shown in Table 8-3.

Table 8-2. Message Posting Loading Sequence

Order	Component	Command	Location
1	Message Posting Bridge	**MP Load Bridge**	Source and Target Server
2	Message Posting Service	**MP Load Service**	Source and Target Workstations
3	Message Posting Notification	**MP Notification**	Source and Target Workstations

Table 8-3. Commands for Loading and Unloading

To	Type	and Press
load Message Posting Bridge	**MP Load Bridge**	GO
unload Message Posting Bridge	**MP Unload Bridge**	GO
load Message Posting Service	**MP Load Service**	GO
unload Message Posting Service	**MP Unload Service**	GO

Creating Messages

Use the following procedure to create a message:

1. Type **MP Notification** on the Executive command line; then press **GO**.

   The Message Posting screen displays (refer to Figure 8-3).

   The cursor displays in the Message Number field, and the default message number assigned to the message is **1**. You can type in a different message number.

2. Press the **TAB** key to move the cursor to the text window. Enter your message. You can enter a four-line message of up to 50 characters per line. You can use the **RETURN** and arrow keys to move the cursor in the text window.

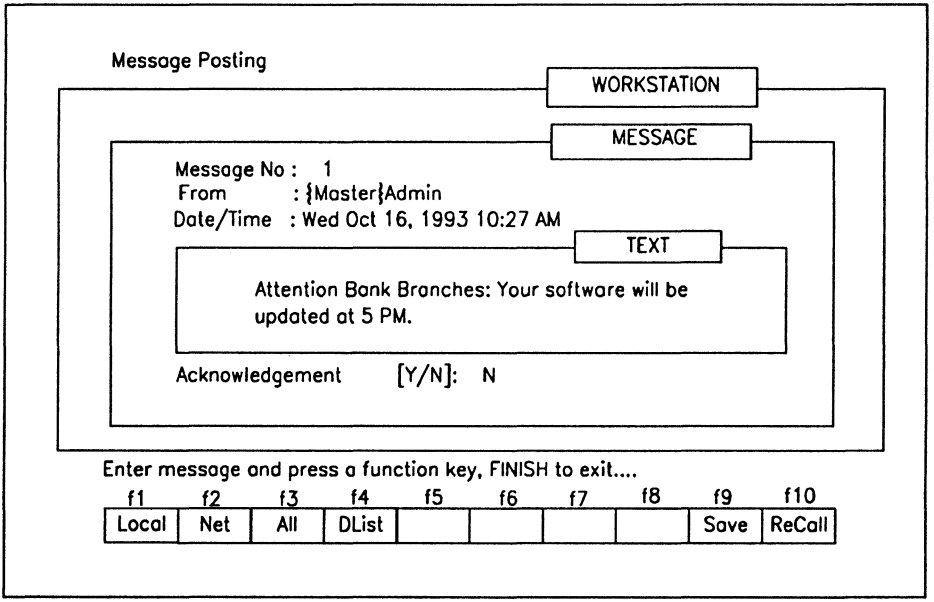
3. If you want to receive an acknowledgement of your message, press the **TAB** key to move the cursor to the acknowledgement field and enter **Y** (Yes).

   The *Acknowledgement Warning* field displays. If you want the system to beep when it receives an acknowledgement, enter **Y** (Yes).

4. Choose one of the following actions:

   - If you want to send the message, refer to Sending Messages in this Section.
   - If you want to save the message and send it at a later time, refer to Saving a Message in this Section.

Figure 8-3. Message Posting Screen


Message Posting
WORKSTATION
MESSAGE
Message No : 1
From : {Master}Admin
Date/Time : Wed Oct 16, 1993 10:27 AM
TEXT
Attention Bank Branches: Your software will be updated at 5 PM.
Acknowledgement [Y/N]: N
Enter message and press a function key, FINISH to exit....
f1 f2 f3 f4 f5 f6 f7 f8 f9 f10
Local Net All DList Save ReCall

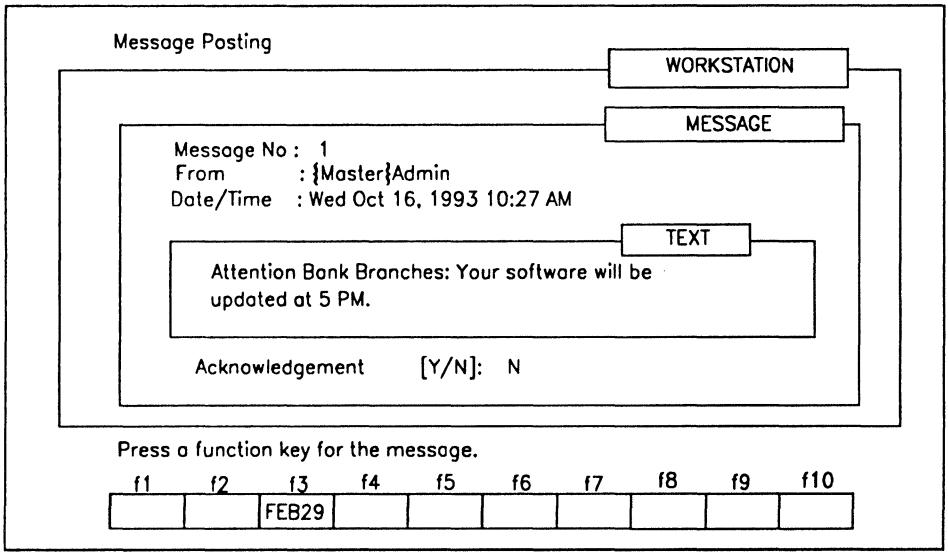
Saving a Message

Use the following procedure if you have composed a message and want to save it and send it later:

1. With your message displayed in the text window of the Message Posting Screen, press **SAVE (F9)**.
2. Press one of the function keys to assign the message to the function key.
3. Type a name in the function key field. For example, you can type **Feb29** for function key **F3**. When you recall the message, you can press **F3** to have the message display.

   Figure 8-4 shows a sample message being saved.

Figure 8-4. Saving a Message


Message Posting
WORKSTATION
MESSAGE
Message No : 1
From : {Master}Admin
Date/Time : Wed Oct 16, 1993 10:27 AM
TEXT
Attention Bank Branches: Your software will be updated at 5 PM.
Acknowledgement [Y/N]: N
Press a function key for the message.
f1 f2 f3 f4 f5 f6 f7 f8 f9 f10
FEB29

Recalling a Saved Message

Use the following procedure to recall a saved message:

1. At the Message Posting Screen, press **ReCall (F10)**.

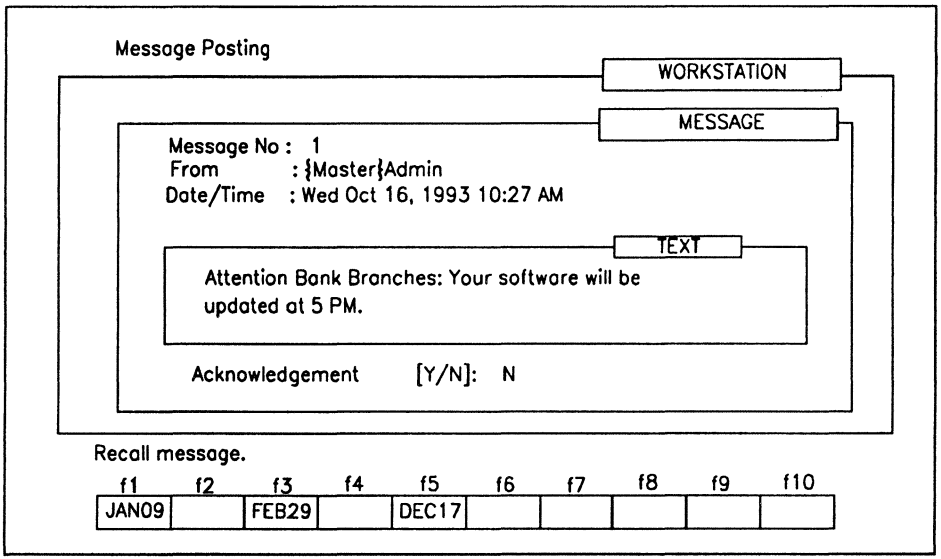
   Figure 8-5 shows a sample message being recalled.

2. Press the function key under which you stored the message.

   The message displays in the text window of the Message Posting Screen.

3. Refer to the appropriate procedure in this section to send the message.

Figure 8-5. Recalling a Message


Message Posting
WORKSTATION
MESSAGE
Message No : 1
From : {Master}Admin
Date/Time : Wed Oct 16, 1993 10:27 AM
TEXT
Attention Bank Branches: Your software will be updated at 5 PM.
Acknowledgement [Y/N]: N
Recall message.
f1 f2 f3 f4 f5 f6 f7 f8 f9 f10
JAN09 FEB29 DEC17

Sending Messages

Use the following procedures to send messages you have created or recalled.

Sending a Message to Other Users on Your Cluster LAN

Use the following procedure to send a message to one user or all users on your local Cluster LAN:

1. With the message you have created or recalled displayed on the Message Posting Screen, press **Local (F1)**.

   The Message Posting User Name Screen displays showing all users to whom you can send a message (refer to Figure 8-6).

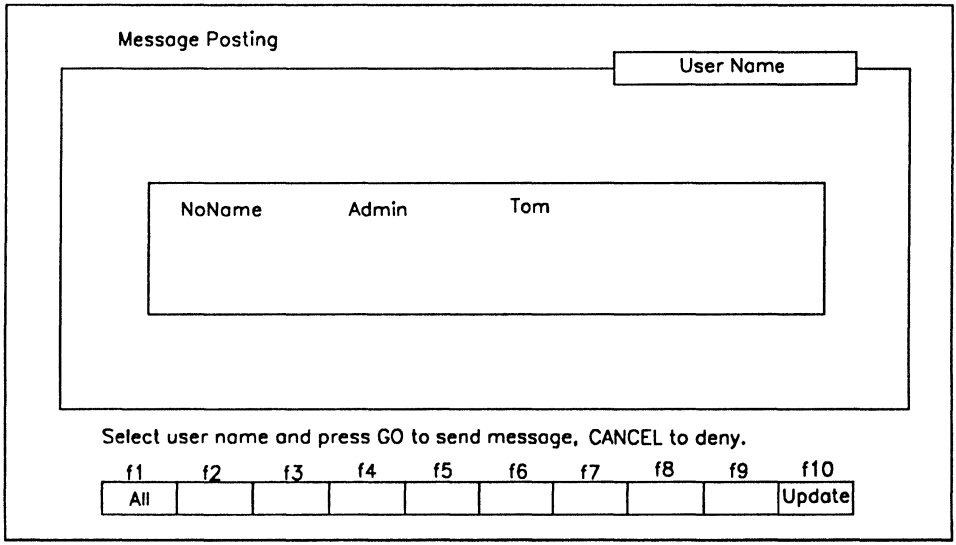
   Note: *Message Posting handles a maximum of 12 characters for each user name. If a user name exceeds 12 characters, the Message Posting User Name Screen displays the first 12 characters only.*

2. Choose one of the following:

   To send the message to a particular user, use the arrow keys to select that user's name; then press **GO**.

   To send the message to all users on the Cluster LAN, press the **All (F1)** key. You can ensure that the list of users displayed is current by pressing **Update (F10)**; then press **GO**.

Figure 8-6. Message Posting User Name Screen



Sending a Message to Users on Other BNet Nodes

Use the following procedure to send a message to one user or all users on another BNet node:

1. With the message you have created or recalled displayed on the Message Posting Screen, press **Net (F2)**.

   A screen displays, prompting you to select BNet.

2. Select BNet.

   The Message Posting Node screen displays with your current node name.

3. Enter the name of the node to which you want to send the message; then press **GO**.

   The Message Posting User Name Screen displays listing the names of all the users on the node.

4. Choose one of the following:

   To send the message to a particular user, use the arrow keys to select that user's name; then press **GO**.

   To send the message to all users on the node, press the **All (F1)** key. You can ensure that the list of users displayed is current by pressing **Update (F10)**; then press **GO**.

Sending a Message to All Users in Your Network

Use the following procedure to send a message to all users on your Cluster LAN and all users on all nodes in your BNet network:

1. Display the message you have created or recalled.
2. Press **All (F3)**.

Sending a Message to the Members of a Distribution List

Use the following procedure to send a message to the members of a distribution list:

1. Using the CTOS Editor, create a distribution list in the path *[Sys]<MP>*.
2. Choose one of the following:
   - To send a message to specific users, enter the node name and user name in the following format:

     NodeName UserName

     Include a space between the node name and the user name, and enter only one node name and user name combination per line.
   - To send a message to all users on a node, enter the node name in the following format:

     NodeName
3. Save and name the distribution list you have created, and exit the Editor.
4. Run the MP notification utility by typing **MP Notification**.
5. Create or recall the message you want to send; then press **DList (F4)**.

   The Distribution List Name field displays.
6. Enter the name of the distribution list; then press **GO**.

Displaying Received Messages and Acknowledgements

When you receive a message or an acknowledgement of a message you sent, your workstation beeps every twenty seconds. You can display a message or acknowledgement in any application you are working in without affecting the application.

Use the following procedure to display a message or acknowledgement:

1. When your workstation begins to beep at twenty-second intervals, press **ACTION+D.**

   A Message window appears displaying the message. If the message is an acknowledgement, an acknowledgement window displays.

2. To close the screen after you have finished reading the message or acknowledgement, press **ACTION+D.**

3. If you receive additional messages or acknowledgements, press **ACTION+D** to view the additional messages or acknowledgements.

   A Message window appears displaying the second message. If the message is an acknowledgement, an acknowledgement window displays.

Note: *You cannot save messages you receive.*

Appendix A
Status Codes

This appendix lists status codes that you may encounter when using RAF.

206	Attempt to load a system service after loading Context Manager
2441	A parameter contains an invalid value
10654	Channel is in use
40205	Message Posting Bridge already loaded
40206	Message Posting Bridge can be loaded on the server only
40207	Message Posting Bridge cannot be loaded after loading CM
40208	Message Posting Bridge was not loaded
40209	Fatal Error
40210	Cannot deinstall Message Posting Bridge after loading CM
40212	Message Posting Service already loaded
40213	Message Posting Service cannot be loaded on XE520/530
40214	Message Posting Service cannot be loaded after loading CM
40215	Message Posting Service was not loaded
40216	Fatal Error

40217	Cannot deinstall Message Posting Service after loading CM
40219	Fatal Error
50035	Device Server not loaded
59872	RAF Target cannot be loaded after Windows
59873	Target User Profile not defined for this Workstation Id
59874	Service cannot be loaded on single partition OS
59875	Service cannot be loaded on an XE520/530 server
59876	R2-S32 Target Interface cannot be loaded before Modem Service
59877	Target has not responded, RS-232 Interface time out
59878	RAF Bridge can only be loaded on the server
59879	RS-232 Target Interface is already loaded for this port
59880	RAF Bridge is already loaded
59881	You must unload RAF Target before loading RAF Bridge
59882	RAF Target is already loaded
59883	PGS is already loaded
59884	RAF Bridge working at full capacity; log On request denied
59885	RAF internal error: contact your local Unisys support Center
59886	Invalid Profile File: File Name
59887	Log File Full: File Name
59888	Log File Error

59889	Queue manager must be installed to support Printer Redirection
59890	Invalid Script file: File Name
59891	User specified in script file is not authorized
59892	Node specified in script file is not accessible
59893	No Targets available on the selected node
59894	Workstation specified in script file doesn't exist
59895	Multiple Targets on selected node; specify one
59896	Password required to load
59897	Log file being used; cannot unload RAF Target
59898	Service cannot be loaded after Context Manager

Section B
RAF Component Worksheet

You can photocopy the component worksheet on the back of this page and fill it out to help you maintain your RAF configuration.

RAF Component Worksheet

Network Location:_____

Network Configuration:_____

Hardware	RAF Source	RAF RS-232 Source	RAF Bridge	RAF Target	RAF RS-232 Target	RAF PGS	Message Posting Notification	Message Posting Service	Message Posting Bridge
Server									
Workstation ID									
Workstation ID									
Workstation ID									
Workstation ID									
Workstation ID									
Workstation ID									
Workstation ID									
Workstation ID									
Workstation ID									
Workstation ID									

Appendix C
Connecting RS-232 Channels

This Appendix contains the following information:

- Typical RS-232 channel specifications
- Direct-connect RS-232-C asynchronous cable specifications

RS-232 Channel Specifications

When you load RAF RS-232 Source, you must specify a channel. Table C-1 lists some typical channel specifications. Refer to your CTOS hardware and operating system manuals for further information.

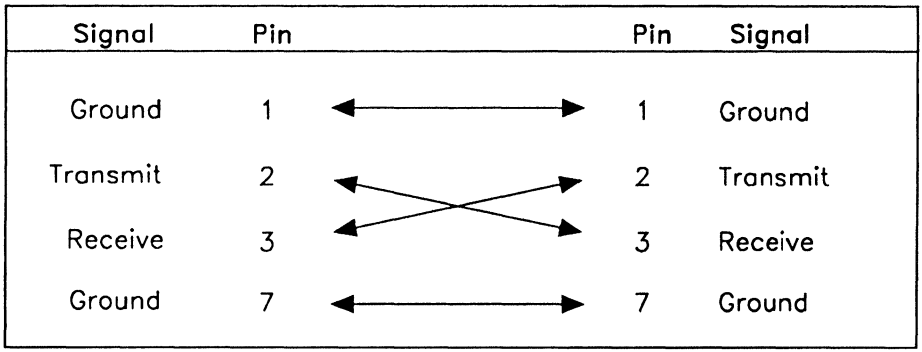
Table C-1. Channel Specifications

Port	Description
[Comm]a	Channel A of workstation, shared resource processor (SRP), or terminal processor (TP) board
[Comm]b	Channel B of workstation, SRP, or TP board
[Comm]c	Channel C, XE520/530, SRP, or TP board
[Comm]d	Channel D, XE520/530, SRP, or TP board
[Comm]1a	Channel A of Multiline Port Expander (first instance)
[Comm]1b	Channel B of Multiline Port Expander (first instance)
[Comm]1c	Channel C of Multiline Port Expander (first instance)
[Comm]1d	Channel D of Multiline Port Expander (first instance)
[Comm]2a	Channel A of Multiline Port Expander (second instance)
[Comm]2b	Channel B of Multiline Port Expander (second instance)
[Comm]2c	Channel C of Multiline Port Expander (second instance)
[Comm]2d	Channel D of Multiline Port Expander (second instance)
[Phone]1	Phone line 1 of voice processor module
[Phone]2	Phone line 2 of voice processor module

Direct Connect RS-232 Cable Wiring

To directly connect two workstations with 25-pin serial connectors, you can use a null-modem cable. This cable crosses pins 2 and 3. Figure C-1 shows the wiring for such a cable.

Figure C-1. Null-Modem Cable Connection



For more information on null-modem and workstation-to-modem connections, refer to the CTOS Modem Service documentation and the documentation for your specific hardware.

Appendix D
Event Reporting

Introduction

This appendix provides information about the systems management event messages that CTOS Remote Access Facility (RAF) software generates. For information about the event message structure, refer to the CTOS InControl event management documentation.

This appendix has two sections:

- CTOS RAF Event Summary - all RAF events listed by application
- CTOS RAF Event Details - detailed reference showing all event fields for each event and suggested remedies

CTOS RAF Event Summary

This section provides summary event information for the following RAF components:

- RAF Source
- RAF Target
- RAF Bridge
- RAF RS-232 Target Interface
- RAF Source/Target User Profile Utilities
- RAF Performance Gathering Service (PGS)
- RAF Message Posting Bridge (MP Bridge)
- RAF Message Posting Service (MP Service)
- RAF Message Posting Terminal

Table D-1. RAF Source Event Summary

Condition	Report ID
Pen ID Range: 1443102721 to 1443102731 (56040001h to 5604000Bh)	
User entered an invalid password	1
User is not authorized to do file transfer	2
Target View/Control is inhibited	3
File access error	4
Fatal error is encountered	5
Modem Server failure	6
PEM server error	7
MCR server error	8
Error occurred during file transfer	9
MCR device access error	10
Successful user logon	11
View session began	12
View session ended	13
Control session began	14
Control sessions ended	15
Control at logon session began	16
Control at logon session ended	17

Table D-2. RAF Target Event Summary

Condition	Report ID
Pen ID Range: 1442906113 to 1442969329 (56010001h to 5601F61Fh)	
Source attempted to redirect MCR without Device Service	1
File access error	2
Fatal error is encountered	3
A user not defined at the Target attempted View/Control	4
User enters an invalid password	5
User access error	6
PEM server error	7
Target View/Control is inhibited	8
Target disables all Sources	9
Target enables all Sources	10
Fatal error occurred during Target installation	11
View session began	12
View session ended	13
Control session began	14
Control sessions ended	15
Control at logon session began	16
Control at logon session ended	17

continued

Table D-2. RAF Target Event Summary (cont.)

Condition	Report ID
User attempted to install Target with Context Manager running	63001
User attempted to install Target on an XE-520 or an XE-530	63002
User attempted to install Target after Window Services is already installed	63003
User attempted to install Target when it is already installed	63004
User attempted to install Target on a single partition operating system	63005
Successful Target installation	63007

Table D-3. RAF Bridge Event Summary

Condition	Report ID
Pen ID Range: 1443037185 to 1443100191 (56030001h to 5603F61Fh)	
Fatal error is encountered	1
User attempted to install Bridge with Context Manager running	63001
User attempted to install Bridge when it is already installed	63004
User attempted to install Bridge on a single partition operating system	63005
Bridge is deinstalled	63006
Successful Bridge installation	63007

Table D-4. RAF RS-232 Target Interface Event Summary

Condition	Report ID
Pen ID Range: 1442971649 to 1443034657 (56020001h to 5602F621h)	
Fatal error is encountered	1
Modem Server error	2
User attempted to install RS-232 Target Interface with Context Manager running	63001
User attempted to install RS-232 Target Interface on a port where it is already installed	63004
User attempted to install RS-232 Target Interface on a single partition-operating system	63005
RS-232 Target Interface is deinstalled	63006
Successful RS-232 Target Interface installation	63007
Failure to install on a port	63008
Modem Service is not installed	63009

Table D-5. RAF Source/Target User Profile Utility Event Summary

Condition	Report ID
Pen ID Range: 1443168257 to 1443168264 (56050001h to 56050008h)	
File access error	1
Successful Admin logon	2
Invalid Admin user or password	3
Admin adds a new user name to RAF profiles	4
Admin modifies a user name in RAF profiles	5
Admin deletes a user name from RAF profiles	6
Admin deletes all user names	7
PEM server error	8

Table D-6. RAF Performance Gathering Service (PGS) Event Summary

Condition	Report ID
Pen ID Range: 1443233793 to 1443296799 (56060001h to 5606F61Fh)	
Fatal error is encountered	1
User attempted to install PGS with Context Manager running	63001
User attempted to install PGS on an XE-520 or an XE-530	63002
User attempted to install PGS when it is already installed	63004
User attempted to install PGS on a single partition operating system	63005
PGS is deinstalled	63006
Successful PGS installation	63007

Table D-7. RAF Message Posting Bridge (MP Bridge) Event Summary

Condition	Report ID
Pen ID Range:1443299329 to 1443362338 (56070001h to 5607F622h)	
Fatal error is encountered	1
User attempted to install MP Bridge with Context Manager running	63001
User attempted to install MP Bridge when it is already installed	63004
User attempted to install MP Bridge on a single partition operating system	63005
MP Bridge is deinstalled	63006
Successful MP Bridge installation	63007
User attempted to install MP Bridge on a workstation that is not the server workstation	63008
MP Bridge is not installed	63009
MP Bridge message file cannot be loaded	63010

Table D-8. RAF Message Posting Service (MP Service) Event Summary

Condition	Report ID
Pen ID Range: 1443364865 to 1443427874 (56080001h to 5608F622h)	
Fatal error is encountered	1
User attempted to install MP Service with Context Manager running	63001
User attempted to install MP Service when it is already installed	63004
User attempted to install MP Service on a single partition operating system	63005
Successful MP Service deinstallation	63006
Successful MP Bridge installation	63007
User attempted to install MP Service on an XE-520 or an XE-530 shared resource processor	63008
MP Service is not installed	63009
MP Service message file cannot be loaded	63010

Table D-9. RAF Message Posting Terminal Event Summary

Condition	Report ID
Pen ID Range: 1443493401 to 1443493404 (5609F619h to 5609F61Ch)	
MP Notification message file cannot be loaded	63001
Operating system error occurred in MP Notification	63004

You should install the Event Manager system service before installing RAF. If an error occurs while RAF is attempting to generate an event, RAF writes the event information to the workstation *Log.sys* file.

RAF Source Event Message Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	1
Context String:	User %V1 failed to logon because of %V2.

Field	Value	Meaning
Class	00000400h	Warning
Topic	0403h	Systems Management, Security, and Control
Activity	50002	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name entered	
%V2	"invalid password" or "unregistered user"	

Advice:	A user attempted to log on with an invalid password or an unregistered user name
Remedy:	Attempt the logon again with a valid password or registered user name

*If RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	2
Context String:	User %V1 not authorized to do file transfer at Target %V2.

Field	Value	Meaning
Class	00000400h	Warning
Topic	0403h	Systems Management, Security, and Control
Activity	50006	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name that attempted a file transfer	
%V2	The name of the Target node	

Advice:	The user is not authorized to perform file transfers to or from the specified Target
Remedy:	Modify the Target user profile to support the transfers; then log on and try again

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020*
Subsystem String:	RAF Source
Report ID:	3
Context String:	User %V1, monitoring inhibited, not allowed to View/Control Target %V2.

Field	Value	Meaning
Class	00000400h	Warning
Topic	0403h	Systems Management, Security, and Control
Activity	50006	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%V2	The name of the Target node	

Advice:	The user is not authorized to view or control the Target
Remedy:	Modify the Target user file and try again

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	4
Context String:	User %V1, erc %S1 encountered when opening %V2

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14000007	General
Component	2000	Nonremovable disk
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned	
%V2	File name	

Advice:	A user cannot open a given RAF critical file
Remedy:	Modify the file name and path and try again

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	5
Context String:	User %V1, fatal error = %S1

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned	

Advice:	Fatal error
Remedy:	Note the error code and contact your designated product support

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF RS-232 Source
Report ID:	6
Context String:	User %V1, Modem server failure, erc = %S1

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0403h	Systems Management, Security, and Control
Activity	8000001	Data Communication General
Component	4006	RS-232 line equipment
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned from Modem Service	

Advice:	RS-232 Source has detected that the connection has been lost
Remedy:	Attempt to redial the connection

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	7
Context String:	User %V1, PEM server error, erc = %S1

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1004	Encryption/decryption device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned from PEM	

Advice:	RAF Source received an error while using the PEM module
Remedy:	Retry

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	8
Context String:	User %V1, MCR server error, erc = %S1

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	3003	Magnetic Card Reader (MCR) device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned from MCR	

Advice:	RAF Source received an error while using the MCR
Remedy:	Retry

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	9
Context String:	User %V1, file transfer terminated with error %S1 at Target %V2

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	2999	Undetermined
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned	
%V2	The name of the Target node	

Advice:	RAF Source encountered an error during a file transfer
Remedy:	Correct the specific error indicated by the error code in the message

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source
Report ID:	10
Context String:	User %V1, erc = %S1 while accessing MCR %V2

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	3003	Magnetic Card Reader device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned	
%V2	The name of the Target node	

Advice:	RAF Source received an error while accessing the MCR
Remedy:	Correct the condition indicated by the error code in the message

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	11
Context String:	User %V1 logged on

Field	Value	Meaning
Class	00000400h	Warning
Topic	0403h	Systems Management, Security, and Control
Activity	50000	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V1	User name	
%S1	Status code returned	
%V2	The name of the Target node	

Advice:	User logged on successfully
Remedy:	None needed

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	12
Context String:	User %V2, view session begin

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50000	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V2	Target user name	

Advice:	A view session has begun with the specified Target user
Remedy:	None needed

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	13
Context String:	User %V2, view session end

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50001	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V2	Target user name	

Advice:	A view session with the specified Target user ended
Remedy:	None needed

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	14
Context String:	User %V2, control session begin

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50000	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V2	Target user name	

Advice:	A control session has begun with the specified Target user
Remedy:	None needed

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	15
Context String:	User %V2, control session end

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50001	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V2	Target user name	

Advice:	A control session with the specified Target user ended
Remedy:	None needed

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	16
Context String:	User %V2, control at logon session begin

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50000	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V2	Target user name	

Advice:	A control at logon session has begun with the specified Target user
Remedy:	None needed

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source)
Subsystem ID:	22020
Subsystem String:	RAF Source*
Report ID:	17
Context String:	User %V2, control at logon session end.

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50001	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFSource.run	
%V2	Target user name	

Advice:	A control at logon session with the specified Target user ended
Remedy:	None needed

*If the RAF is running over the RS-232 interface, the event message SubSystem is RS232 Source.

RAF Target Event Message Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	1
Context String:	Device server must be installed on Target %V1 for MCR redirection

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V1	The name of the Target node	

Advice:	A controller attempted to redirect the MCR on the Target when Device Service was not installed on the Target
Remedy:	Install Device Service on the Target

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	2
Context String:	Erc = %S1 encountered by Target %V1 when opening file %V2

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	2000	Nonremovable disk
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%S1	Status code returned from the Target node	
%V1	The name of the Target node	
%V2	The name of the file	

Advice:	RAF Target encountered an error while the user was opening a file
Remedy:	Correct the condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	3
Context String:	Fatal error: %S1, waiting to be deinstalled

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFDeinstallTarget.run	
%S1	Status code returned from the Target node	

Advice:	Fatal error
Remedy:	If possible, unload RAF Target. Correct the condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	4
Context String:	User %V2 not defined at Target %V1, cannot View/Control

Field	Value	Meaning
Class	00000400h	Warning
Topic	0403h	Systems Management, Security, and Control
Activity	50006	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	User name	
%V1	The name of the Target node	

Advice:	Target user profile does not contain an entry for this user
Remedy:	Add the user to the Target user profile and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	5
Context String:	User %V2, invalid password at Target %V1, access denied

Field	Value	Meaning
Class	00000400h	Warning
Topic	0403h	Systems Management, Security, and Control
Activity	50006	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	User name	
%V1	The name of the Target node	

Advice:	Source user attempted to log on with an invalid password
Remedy:	Log on with correct password, or modify the Target user profile

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	6
Context String:	Access denied to user %V2; Target %V1 not on Logon screen

Field	Value	Meaning
Class	00000400h	Warning
Topic	0403h	Systems Management, Security, and Control
Activity	50006	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	Source user name	
%V1	The name of the Target node	

Advice:	The specified Source user tried to access the specified Target; however, the Target access authorization was set to Control at Logon and the Target workstation was not on the logon screen
Remedy:	Log out the Target user and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	7
Context String:	Target %V1, PEM server error, erc = %S1

Field	Value	Meaning
Class	00000400h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	3003	Magnetic card reader device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V1	The name of the Target node	
%S1	Status code returned from the Target node	

Advice:	RAF Target encountered an error while using the PEM
Remedy:	Correct the condition indicated by the error code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	8
Context String:	Target %V1, View/Control inhibited

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V1	The name of the Target node	

Advice:	The Source user is not authorized to view or control this workstation
Remedy:	Modify the Source user's privileges in the Target user profile

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	9
Context String:	All Sources disabled by Target %V1

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V1	The name of the Target node	

Advice:	The specified Target node has disabled monitoring for all Source users
Remedy:	Enable Source monitoring; the press **ACTION+M** to try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	10
Context String:	All Sources enabled by Target %V1

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V1	The name of the Target node	

Advice:	A user at the specified Target node has enabled monitoring for all Source users
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	11
Context String:	Fatal error: %S1, cannot install Target.

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%S1	Status code returned from the Target node	

Advice:	RAF Target could not be installed
Remedy:	Correct the condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	12
Context String:	User %V2, view session begin

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50000	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	Source user name	

Advice:	A view session has begun with the specified Source user
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	13
Context String:	User %V2, view session end

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50001	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	Source user name	

Advice:	A view session with the specified Source user ended
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	14
Context String:	User %V2, control session begin

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50000	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	Source user name	

Advice:	A control session has begun with the specified Source user
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	15
Context String:	User %V2, control session end

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50001	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	Source user name	

Advice:	A control session with the specified Source user ended
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	16
Context String:	User %V2, control at logon session begin

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50000	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	Source user name	

Advice:	A control at logon session has begun with the specified Source user
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	17
Context String:	User %V2, control at logon session end

Field	Value	Meaning
Class	00000100h	Normal
Topic	0403h	Systems Management, Security, and Control
Activity	50001	Security General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V2	Source user name	

Advice:	A control at logon session with the specified Source user ended
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	63001
Context String:	Cannot be installed when Context Manager is running

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	

Advice:	User attempted to install RAF Target while Context Manager was running
Remedy:	Exit from Context Manager; then load RAF Target

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	63002
Context String:	Cannot be installed on an XE-520 or an XE-530

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	

Advice:	User attempted to install RAF Target on an XE-520 or XE-530
Remedy:	None; this is an unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	63003
Context String:	Cannot be installed after Window service

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
Source Module		

Advice:	User attempted to install RAF Target while Window Services was running
Remedy:	Terminate Window Services; then load RAF Target

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	63004
Context String:	Already installed

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	

Advice:	User attempted to load RAF Target on a workstation in which RAF Target is already loaded
Remedy:	To use a different workstation ID, unload RAF Target and reload it with the new ID; otherwise, no action is needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	63005
Context String:	Cannot be installed on a single partition OS

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	

Advice:	User attempted to install RAF Target on a single-partition operating system
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	63006
Context String:	Target %V1 deinstalled

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFDeinstallTarget.run	
%V1	The name of the Target node	

Advice:	RAF Target was successfully unloaded from memory
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Target)
Subsystem ID:	22017
Subsystem String:	RAF Target
Report ID:	63007
Context String:	Target %V1 successfully installed

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFTarget.run	
%V1	The name of the Target node	

Advice:	RAF Target installed successfully
Remedy:	None needed

RAF Bridge Event Message Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Bridge)
Subsystem ID:	22019
Subsystem String:	RAF Bridge
Report ID:	1
Context String:	Fatal error: %S1, waiting to be deinstalled

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFBridge.run	
%S1	Status code returned	

Advice:	Fatal error
Remedy:	Correct condition indicated in error code

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Bridge)
Subsystem ID:	22019
Subsystem String:	RAF Bridge
Report ID:	63001
Context String:	Cannot be installed when Context Manager is running

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFBridge.run	

Advice:	User attempted to load RAF Bridge while Context Manager was running
Remedy:	Exit from Context Manager; then load RAF Bridge

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Bridge)
Subsystem ID:	22019
Subsystem String:	RAF Bridge
Report ID:	63004
Context String:	Already installed

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFBridge.run	

Advice:	User attempted to load RAF Bridge when it was already loaded
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Bridge)
Subsystem ID:	22019
Subsystem String:	RAF Bridge
Report ID:	63005
Context String:	Cannot be installed on a single partition OS

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFBridge.run	

Advice:	User attempted to load RAF Bridge on a single-partition operating system
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Bridge)
Subsystem ID:	22019
Subsystem String:	RAF Bridge
Report ID:	63006
Context String:	RAF Bridge deinstalled

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFDeinstallBridge.run	

Advice:	RAF Bridge successfully unloaded from memory
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Bridge)
Subsystem ID:	22019
Subsystem String:	RAF Bridge
Report ID:	63007
Context String:	Successfully installed

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFBridge.run	

Advice:	RAF Bridge was successfully loaded in memory
Remedy:	None needed

RAF RS-232 Target Interface Event Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	1
Context String:	RS-232 Interface serving port %V1, fatal error: %S1, waiting to be deinstalled

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	
%V1	The name of the port	
%S1	Status code returned	

Advice:	The RS-232 Target Interface detected a fatal error and is waiting to be unloaded
Remedy:	If possible, unload the RS-232 Target Interface. Correct the error condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	2
Context String:	RS-232 Interface serving port %V1, Modem Server failure, erc = %S1, dropping line

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	
%V1	The name of the port	
%S1	Status code returned by the Modem Service	

Advice:	The RS-232 Target Interface received a failure message from the Modem Service and is breaking the connection
Remedy:	Correct the problem indicated in the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	63001
Context String:	Cannot be installed when Context Window Manager is running

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	

Advice:	User attempted to load RS-232 Target Interface while Context Manager was running
Remedy:	Exit from Context Manager; then load RS-232 Target Interface

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	63004
Context String:	Already installed on Port %V1

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	
%V1	The name of the port	

Advice:	User attempted to load RS-232 Interface on a port that already has RS-232 Interface loaded
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	63005
Context String:	Cannot be installed on a single partition OS

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	

Advice:	User attempted to load RS-232 Target on a single-partition operation system
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	63006
Context String:	RS-232 Interface serving port %V1 deinstalled

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	DeinstallRS232Target.run	
%V1	The name of the port	

Advice:	RS-232 Interface serving the specified port was successfully deinstalled
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	63007
Context String:	Successfully installed to serve port %V1

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	
%V1	The name of the port	

Advice:	RS-232 Target Interface Service was successfully loaded to serve the specified port
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	63008
Context String:	Erc %S1, cannot install on Port %V1

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	
%S1	Status code returned	
%V1	The name of the port	

Advice:	RS-232 Target Interface was unable to load for the specified port
Remedy:	Correct the condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF RS-232 Target Interface)
Subsystem ID:	22018
Subsystem String:	RS232 Target Interface Server
Report ID:	63009
Context String:	Modem Service not installed, cannot install

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RS232Target.run	

Advice:	User attempted to load the RS-232 Target Interface before loading the Modem Service
Remedy:	Load the Modem Service and try again

RAF Source/Target User Profile Utility Event Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	1
Context String:	Erc = %S1, while accessing File = %V2

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%S1	Status code returned	
%V2	The name of the file RAF Profile was accessing	

Advice:	The RAF Source Profile utility encountered an error while accessing the specified file
Remedy:	Correct the error condition indicated by the status code and try again

* If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	2
Context String:	Admin %V1 logged on for %V2 profile management

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%V1	Admin user name	
%V2	The name of the source or Target node	

Advice:	The named administrator has logged onto the utility to manage profiles for the specified node
Remedy:	None needed

* If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	3
Context String:	Admin %V1 failed to logon because of %V2

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%V1	Admin user name	
%V2	Invalid user name or password	

Advice:	The administrator was unable to log on because the user name or password was invalid
Remedy:	Log on with a correct user name or password

* If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	4
Context String:	Admin %V1, Created a new user %V2 with level %V3

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%V1	Admin user name	
%V2	New user name added to the RAF profiles	
%V3	Authority level assigned to the new user name	

Advice:	The specified administrator created the new user indicated in the message
Remedy:	None needed

*If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	5
Context String:	Admin %V1, Modified user %V2, level %V3

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%V1	Admin user name	
%V2	User name modified in the RAF profiles	
%V3	Authority level of the modified user name	

Advice:	The specified administrator modified the user profile as indicated in the message
Remedy:	None needed

*If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	6
Context String:	Admin %V1, Deleted user %V2

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%V1	Admin user name	
%V2	User name deleted from the RAF profiles	

Advice:	The specified administrator deleted the profile for the specified user
Remedy:	None needed

*If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	7
Context String:	Admin %V1, Deleted all users

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%V1	Admin user name	

Advice:	The specified administrator deleted all the users
Remedy:	None needed

*If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Source/Target User Profile)
Subsystem ID:	22021
Subsystem String:	RAF Source Profile*
Report ID:	8
Context String:	Admin %V1, PEM Server error - %S1

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1004	Encryption/decryption device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	RAFProfile.run	
%V1	Admin user name	
%S1	Status code returned by the PEM service	

Advice:	RAF Profile detected an error from the PEM Service while the specified administrator was logged on
Remedy:	Correct the condition indicated by the status code and try again

*If the **RAF Target User Profile** command is running, the event message SubSystem is RAF Target Profile.

Performance Gathering Service (PGS) Event Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Performance Gathering Statistics)
Subsystem ID:	22022
Subsystem String:	RAF PGS
Report ID:	1
Context String:	Fatal error: %S1, waiting to be deinstalled

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0501h	Security, Control, and Statistics
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1400	Statistics
Operator Generated Flag	FALSE	Generated by application
Run File Name	PGS.run	
%S1	Status code returned	

Advice:	PGS encountered a fatal error
Remedy:	If possible, unload PGS. Correct the condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Performance Gathering Statistics)
Subsystem ID:	22022
Subsystem String:	RAF PGS
Report ID:	63001
Context String:	Cannot be installed when Context Manager is running

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0501h	Security, Control, and Statistics
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1400	Statistics
Operator Generated Flag	FALSE	Generated by application
Run File Name	PGS.run	

Advice:	User attempted to load PGS while Context Manager was running
Remedy:	Exit from Context Manager; then load PGS

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Performance Gathering Statistics)
Subsystem ID:	22022
Subsystem String:	RAF PGS
Report ID:	63002
Context String:	Cannot be installed on an XE-520/530

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0501h	Security, Control, and Statistics
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1400	Statistics
Operator Generated Flag	FALSE	Generated by application
Run File Name	PGS.run	

Advice:	User attempted to load PGS on and XE-520 or XE-530
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Performance Gathering Statistics)
Subsystem ID:	22022
Subsystem String:	RAF PGS
Report ID:	63004
Context String:	Already installed

Field	Value	Meaning
Class	00000400h	Warning
Topic	0501h	Security, Control, and Statistics
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1400	Statistics
Operator Generated Flag	FALSE	Generated by application
Run File Name	PGS.run	
Source Module		

Advice:	User attempted to load PGS when it was already loaded
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Performance Gathering Statistics)
Subsystem ID:	22022
Subsystem String:	RAF PGS
Report ID:	63005
Context String:	Cannot be installed on a single partition OS

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0501h	Security, Control, and Statistics
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1400	Statistics
Operator Generated Flag	FALSE	Generated by application
Run File Name	PGS.run	

Advice:	User attempted to load PGS on a single-partition operating system
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Performance Gathering Statistics)
Subsystem ID:	22022
Subsystem String:	RAF PGS
Report ID:	63006
Context String:	PGS deinstalled

Field	Value	Meaning
Class	00000400h	Warning
Topic	0501h	Security, Control, and Statistics
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1400	Statistics
Operator Generated Flag	FALSE	Generated by application
Run File Name	DeinstallPGS.run	

Advice:	PGS was successfully unloaded from memory
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (RAF Performance Gathering Statistics)
Subsystem ID:	22022
Subsystem String:	RAF PGS
Report ID:	63007
Context String:	Successfully installed

Field	Value	Meaning
Class	00000100h	Normal
Topic	0501h	Security, Control, and Statistics
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1400	Statistics
Operator Generated Flag	FALSE	Generated by application
Run File Name	PGS.run	

Advice:	PGS was successfully loaded into memory
Remedy:	None needed

Message Posting (MP) Bridge Event Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	1
Context String:	Fatal error: %S1, in MP Bridge, waiting to be deinstalled

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPBrdg.run	
%S1	Status code returned from Message Posting Bridge	

Advice:	MP Bridge encountered a fatal error
Remedy:	If possible, unload the MP Bridge service. Correct the condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63001
Context String:	MP Bridge cannot be installed when CM is running

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPBrdg.run	

Advice:	User attempted to load MP Bridge while Context Manager was running
Remedy:	Exit from Context Manager; then load MP Bridge

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63004
Context String:	MP Bridge already installed

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPBrdg.run	

Advice:	User attempted to load MP Bridge when it was already loaded
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63005
Context String:	MP Bridge cannot be installed on a single partition OS

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPBrdg.run	

Advice:	User attempted to load MP Bridge on a single-partition operating system
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63006
Context String:	MP Bridge successfully deinstalled

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	DeinstMPBrdg.run	

Advice:	MP Bridge was successfully unloaded from memory
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63007
Context String:	MP Bridge successfully installed

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPBrdg.run	

Advice:	MP Bridge was successfully loaded into memory
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63008
Context String:	MP Bridge can only be loaded on the server

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPBrdg.run	

Advice:	User attempted to load MP Bridge on a cluster workstation
Remedy:	Load MP Bridge on the server; MP Bridge on a cluster workstation is an unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63009
Context String:	MP Bridge is not installed

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	

Advice:	User attempted to install MP Server when MP Bridge was not installed
Remedy:	Install MP Bridge and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Bridge)
Subsystem ID:	22023
Subsystem String:	MESSAGE POSTING
Report ID:	63010
Context String:	Cannot load MP Bridge message file

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPBrdg.run	

Advice:	MP Bridge could not load its message file, *MPBrdg.msg*
Remedy:	Reinstall the Message Posting software from the distribution diskettes and try again

Message Posting (MP) Service Event Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	1
Context String:	Fatal error: %S1, in MP Service, waiting to be deinstalled

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	
%S1	Status code returned from the Message Posting Service	

Advice:	MP Service detected a fatal error
Remedy:	If possible, unload the MP Service. Correct the error condition indicated by the status code and try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63001
Context String:	MP Service cannot be installed when CM is running

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	

Advice:	User attempted to load MP Service while Context Manager was running
Remedy:	Exit from Context Manager; then load MP Service

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63004
Context String:	MP Service already installed

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	

Advice:	User attempted to load MP Service when it was already loaded
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63005
Context String:	MP Service cannot be installed on a single partition OS

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	

Advice:	User attempted to install the MP Service on a single-partition operating system
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63006
Context String:	MP Service successfully deinstalled

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	DeinstMpSrvr.run	

Advice:	MP Service was successfully unloaded from memory
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63007
Context String:	MP Service successfully installed

Field	Value	Meaning
Class	00000100h	Normal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	

Advice:	MP Service was successfully loaded into memory
Remedy:	None needed

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63008
Context String:	MP Service cannot be loaded on an XE-520/530

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	

Advice:	User attempted to load the MP Service on an XE-520 or an XE-530
Remedy:	None; unsupported configuration

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63009
Context String:	MP Service is not installed

Field	Value	Meaning
Class	00000400h	Warning
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPTerm.run	

Advice:	User attempted to use MP Terminal when MP Service was not installed
Remedy:	Install MP Service; then try again

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Service)
Subsystem ID:	22024
Subsystem String:	MESSAGE POSTING
Report ID:	63010
Context String:	Cannot load MP Service message file

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPSrvr.run	

Advice:	MP Service was unable to load its message file, *MPSrvr.msg*
Remedy:	Reinstall Message Posting from the distribution media; then try again

Message Posting (MP) Terminal Event Details

Event Message Documentation Form

Product Name:	CTOS Remote Access Facility (Message Posting Terminal)
Subsystem ID:	22025
Subsystem String:	MESSAGE POSTING
Report ID:	63001
Context String:	Cannot load MP Notification message file

Field	Value	Meaning
Class	00002000h	Fatal
Topic	0401h	Security and Control
Activity	14049999	General
Component	1000	Primary CPU device
SubTopic	1800	Control
Operator Generated Flag	FALSE	Generated by application
Run File Name	MPTerm.run	

Advice:	MP Terminal could not open its message file, *MPTerm.msg*
Remedy:	Reinstall Message Posting from the distribution diskettes; then try again

Glossary

A

Action keys

When pressing the **ACTION** key and another key at the same time, both keys produce a function. For example, **ACTION+CANCEL.**

application partition

A partition of user memory in a workstation. There can be one or more partitions, each containing an executable program.

asynchronous

A lack of timing relationship between bits, characters, and events. Characters are transmitted in a variable timing interval through use of start and stop bits.

B

background

A process or program that is independent of any foreground process.

Burroughs Network Architecture (BNA)

A Unisys proprietary network architecture for A and V Series mainframes that provides lower OSI layer services, including specialized features and functionality.

BNET

A Unisys network software program that is commonly referred to as classic BNET since it is the precursor to BNet II. BNET provides limited communication services between Cluster LANs. BNET does not provide access to OSI services. *See BNet II.*

BNet II

A Unisys network software program allowing users of CTOS systems to access the files and other resources of systems between Cluster LANs.

Bridge

See RAF Bridge.

C

central processing unit (CPU)

A computer unit that contains circuits and controls the interpretation and execution of instructions.

channel

An RS-232-C communications port on a workstation or XE520/XE530.

cluster

A local resource-sharing network connecting a server and one or more cluster workstations. Each workstation contains an RS-422 or RS-485 channel for cluster cable connections.

control

A monitoring mode in which a Source user views a Target workstation and can use its computing resources.

CPU

See central processing unit.

D

dial-up connection

A connection over a switched line, usually a telephone line, rather than a direct cable connection.

DCA

A Unisys proprietary network architecture for 1100/2200 mainframes that provides lower OSI layer services, including specialized features and functionality. *See Open Systems Interconnect (OSI), BNA, and SNA.*

E

encryption

A conversion of plain text into an unintelligible form. *See PEM Encryption.*

Ethernet LAN

A local-area networking protocol, defined by the IEEE standard 802.3, that allows stations to listen before transmitting. A transmitting station detecting a collission terminates its transmission.

event

A significant occurrence which requires special processing. *See InControl.*

Executive

An interactive application program receiving commands from a user and requesting the operating system to load programs and services to execute the commands.

F

file specification

A file identifier that, in its expanded form, can include a node name, volume name, directory name, file prefix, and a file name.

I

InControl

A suite of CTOS products that provides systems management facilities. The facilities are distributed throughout the network for observation, monitoring, command, and control of distributed CTOS hardware and software.

Interactive Performance Monitor (IPM)

An interactive program within RAF Source and RAF RS-232 Source that displays a Target's CPU status at current, average, or elapsed time intervals.

interconnect

To link computers so that they can transmit and receive electronic signals.

interoperate

The successful exchange and interpretation of data between computers or programs as well as the correct response to that data.

IPM

See Interactive Performance Monitor.

L

LEM

See Local Event Management .

load

A process activating a program or service that stays resident in memory.

local area network (LAN)

A network in a limited geographical area, connecting two or more computers using a common communications protocol for sharing information and resources.

Local Event Management

Local Event Management is a CTOS application that collects and conveys messages about system problems and conditions (events) of potential interest to those who interface with it. It provides a mechanism for system processes, programs, services, or applications to generate and receive event messages between workstations in a cluster network.

M

MCR

See magnetic card reader.

magnetic card reader (MCR)

A device that reads data from the magnetic surface of a plastic card to a computer.

Message Posting

An interactive program for creating, sending, retrieving, or storing messages.

Message Posting Bridge

A system service for transporting messages in a Cluster LAN. It is loaded on the cluster server.

Message Posting Service

A system service used for receiving messages at the destination.

Modem Service

A Unisys communications software program that provides the routines to establish connections between computers and modems over directly-connected asynchronous lines or through the switched telephone network.

N

network

A combination of computers, peripheral devices, and circuits that are interconnected.

node

A server workstation in a local area network. Node also refers to the first element of a full file specification.

O

Open Systems Interconnect (OSI)

A set of standards defined by the International Standards Organization (ISO) that, when implemented, allow different computer systems to communicate with each other. *See OSI Reference Model.*

OSI Reference Model

A seven-layer model that provides the framework for building an open network. The seven layers are: Upper Layers include Application, Presentation, and Session; Lower Layers include Transport, Network, Data Link, and Physical.

P

packet-switched network

A network transmitting data in packets using the X.25 protocol. The packets can be routed individually and reassembled to form a complete message at the destination.

parameter

A program option that is specified by the user.

partition

A logical part of memory allocated to the operating system or an application system. The memory can be divided into several partitions varying in size.

PEM

See Peripheral Extension Module.

PEM Encryption

Encryption of RAF passwords using a Peripheral Extension Module with encryption option based on the DES standard.

PGS

See Performance Gathering Service.

Performance Gathering Service (PGS)

A system service that gathers Target CPU activity data and transfers this information to the Interactive Performance Monitor for display.

Peripheral Extension Module (PEM)

A device connected to a workstation that implements encryption of passwords and allows attachment of RS-232 peripherals.

platform

A specific configuration of hardware, operating system, and presentation environment. Examples include a PW2 workstation running MS-DOS with Windows, a U6000 workstation running UNIX and Motif, and an SG5000 workstation running CTOS and Presentation Manager.

protocol

A set of rules defining network functionality. There are open and proprietary networking protocols.

Public-Switched Telephone Network (PSTN)

A public telephone network comprised of regional, local, and independent telephone companies all interconnected.

R

RAF

See Remote Access Facility.

RAF Bridge

A system service transporting RAF requests to a Target workstation in a cluster. RAF Bridge is loaded on the cluster server.

RAF Source

An interactive program for viewing, controlling, or scanning another workstation.

RAF Target

A system service supporting viewing, controlling, or scanning of the workstation on which it is loaded.

RAF User Profile Utilities

Two utilities, RAF Source User Profile and RAF Target User Profile, that define user names, passwords, security level, and MCR data.

RAF RS-232 Target Interface Service

A system service used by a RAF Target to communicate with the RAF RS-232 Source over a Modem Service network. RAF RS-232 Target Interface Service is loaded on the Target workstation or server to provide access to all Targets in a Cluster LAN.

Remote Access Facility (RAF)

A Unisys software program allowing a workstation to view, control, or scan another local or remote workstation.

RS-232-C connection

A standard, defined by the Electronics Industry Association (EIA), that specifies the rules by which data is moved across a physical interface between a workstation (data terminal equipment) and a modem (data communications equipment).

S

scan

The capability to view a snapshot of each Target workstation in a Cluster LAN or each partition within a workstation.

server

A workstation or shared resource processor serving as the hub for cluster communications.

Shared Resource Processor

A multiprocessor, floor-standing CTOS server. The shared resource processor can run various programs on each of the processors. It can hold up to six processor boards.

SNA

See Systems Network Architecture.

Source

The workstation that views, controls, or scans another workstation or shared resource processor.

SuperGen

A Unisys series of workstations that employ or are modelled after Personal Computer (PC) architecure.

Systems Network Architecture (SNA)

An IBM proprietary network architecture that standardizes the virtual telecommunication access method (VTAM) and the network control program (NCP).

T

Target

A workstation or XE530 being viewed, controlled, or scanned by another workstation.

token ring

A LAN protocol defined by the IEEE 802.5 standard. A token ring uses a token (a packet of control information) to control access to the LAN.

V

view

The capability of a Target workstation's screen to display on a Source workstation.

W

WAN

See Wide Area Network.

Wide Area Network (WAN)

A public or private data and voice network serving a wide geographical area.

X

X.25

A packet-switched network protocol based on a standard developed by the International Telegraph and Telephone Consultative Committee (CCITT).

XE520/XE530

See Shared Resource Processor.

Index

%V1, D-9
%V2, D-9
1100/2200 Series connections, 3-9
:ActionQuote: parameter, 2-7
:BlockKeysTimeout: parameter, 2-7
:NoOfSendKeys: parameter, 2-7
:Notification: parameter, 2-8
:NotifyBlink: parameter, 2-8
:RS232TimeOut: parameter, 2-7
:SourceTimeOut: parameter, 2-7
:SzVidUpdateBuffer: parameter, 2-8
:WrapLogFileAllowed: parameter, 2-8

A

A Series mainframe connections, 3-8
About This Guide, xv
access levels in RAF, 1-6, 4-3
access to Source and Target, 4-1
accessing the view mode, 7-15
acknowledgements for messages, 8-11
ACTION + KEY combinations, xx
ACTION + ', xix
Action keys
  control mode, 7-18
  for Target, 7-24
  remote debugging, 7-20
  scan mode, 7-21
  view mode, 7-16
:ActionQuote: parameter, 2-7
activity for CPU displayed, 7-13
activity of CPU on Target, 7-12
activity component of events, D-9
Administration form for Target user profile, 4-11
administration name change
  in Source user profile, 4-5
  in Target user profile, 4-11
administrator default name, 4-4
administrator's use of this guide, xv
advice for RAF problems, D-10
amount of time without Source activity, 7-7
Application Automator (AA), 6-2
application debugging, 7-14
asynchronous transmission, 1-1
average CPU use, 7-23

B

basic component configuration, 1-2
beep redirection, 1-6
:BlockKeysTimeout: parameter, 2-7
BNA
  communications to mainframe, 3-8
  definition, 3-1
BNET
  basic configuration in RAF, 1-4
  components on Source/Target workstations, 3-11
  with Modem Service, 6-3

BNet II
components, 3-6
network, 3-2
network components, 3-5
network definition, xix
node definition, 3-1
protocol, 1-3
with Message Posting, 8-2
BNet II or BNET references, xx
Bridge (RAF component), 1-8
Burroughs Network Architecture (BNA), 3-1

C

cable
wiring for null-modem cable, C-3
capabilities of RAF, 1-6
changing
Administrator name in Target user profile, 4-11
password in Target user profile, 4-11
Source administration name, 4-5
video update time interval, 7-25
channel specification in script file, 4-16
channel specifications, C-1
character positions on magnetic card strip, 4-8
characters in an MP message, 8-1
character-mapped mouse cursor, 6-3
checking
errors in transmission, 7-6
passwords, 4-2
Chit-Chat
Action key, 7-24
conditions for use, 7-33
general, 1-6
using, 7-33
screen, 7-34
class, D-9
classic BNET
network, 3-2
protocol, 1-3
cluster access definition, 3-1
cluster configuration
definition, xix
with RAF, 1-2
cluster definition, 2-1
cluster installation of RAF from a server, 2-6
Cluster LAN
network configuration, 3-2,
on Source and Target workstations, 3-11
with Message Posting, 8-2
with RAF, 1-3
cluster workstation,
definition, xix
codes
status, A-1
commands to load/unload Message Posting, 8-4
communication networks for RAF, 3-1
communication ports on workstations, C-2
compatible hardware for RAF, 1-2
component worksheet, 3-12, B-1
component, D-9

components
for Message Posting, 8-3
of RAF to install, 2-3
RAF, 1-8
concurrent sessions, 6-4
configurable keystroke transmission, 1-7
configuration
documenting on a worksheet, B-1
general RAF layout, 1-2
sample for RAF recording, 7-28
configuration file
customization, 1-6
for RAF, 2-6
parameters, 2-7
configuring
ACTION + ', xix
BNet parameters with Message Posting, 8-3
RAFConfig.sys file, 2-6
RAF networks, 3-1
RAF Telephone Directory, 5-1
connecting
RS-232 channels, C-1
to a Target, 7-2
to a mainframe, 3-8
to a Target through script files, 4-15
two workstations directly, C-3
connection for null-modem cable, C-3
contents of this guide, xv
Context Manager, 6-2
context string, D-9
Context/Window Manager references, xx
Control at Logon privilege, 4-3
control mode of monitoring, 7-14, 7-17
control notification, 1-6, 6-6
control session
starting, 7-17
general, 7-13
Control Workstation privilege, 4-3
controlling a Target workstation, 7-12
conventions, xviii
CPU activity displayed, 7-13
CPU status, 7-22
CPU use
current, 7-23
average, 7-23
elapsed, 7-23
Create Profile menu, 4-6
creating
a Magnetic Card Reader (MCR) profile, 4-7
an MCR profile, 4-5
a Source user profile, 4-5
a Target user profile, 4-12
a Telephone Directory for RAF, 5-1
script files, 4-15
Source/Target user profiles, 4-1
Target user profile, 4-10
user profiles, 4-4
CTOS cluster configuration, 1-2
CTOS cluster LAN, 3-2,
CTOS Debugger, 7-12
CTOS InControl, xx
CTOS publications, xx
CTOS RAF event summary, D-1
CTOS versions, 2-4
CTOS Windows Services, 6-2
CTOS workstations used with RAF, xix, 1-2

current CPU use, 7-23
custmomizeable configuration file, 1-6
customizing the RAF environment, 4-1

D

Data Encryption Standard (DES), 4-14
data transmission errors, 7-6
DCA definition, 3-1
debug privileges, 4-3
debugger, 7-12
debugging remote, 1-6, 7-19
default
  administrator name in profile utility, 4-4
  password for Source user profile, 4-4
defining
  access to RAF Source and Target, 4-1
  a log file, 4-13
definitions
  BNA, 3-1
  BNet node, 3-1
  cluster, 2-1
  cluster access, 3-1
  DCA, 3-1
  in overview, 1-1
  LAN, 1-1
  install, 2-1
  installation and configuration, 2-1
  load, 2-1
  local system, 2-1
  network, 3-1
  networking, 3-1
definitions (continued)
  of RAF, 1-2
  OSI, 3-1
  OSI Transport LAN, 3-2
  packet-switched network, 1-1
  protocol, 3-2
  server, 2-1
  Source, 2-1
  Target, 2-1
  terms used in this guide, xix
  WAN, 1-1
  X.25, 3-2
deleting
  a Source user profile, 4-7
  a Target user profile, 4-13
  a Telephone Directory, 5-2
description
  events, D-1
  of RAF, 1-2
details for Message Posting
  Bridge event messages, D-87
  Service event messages, D-96
  Terminal event messages, D-105
details of
  RAF PGS event messages, D-80
  RAF Source/Target user profile event messages, D-69
  RAF Bridge event messages, D-54
  RAF RS-232 Target Interface event messages, D-60
  RAF Target event messages, D-30
detection of monitoring, 1-6
determining installation command, 2-2
Device Service
  loading, 6-2
  references, xx

diagrams presented in this guide, xix
dialog feature, 1-6
dial-up
  connection, 1-7
  connectivity, 3-10
  menu, 7-9
direct connect RS-232 cable wiring, C-3
Directory (telephone), 1-8
disabling security, 4-2
displaying CPU
  activity, 7-12
  status, 7-22
displaying
  IPM information, 7-22
  messages and acknowledgements, 8-11
  Target screen on Source, 7-12
  the Targets available, 7-10
Distributed Communications Architecture (DCA), 3-1
distribution lists for message sending, 8-11
documenting network, 3-12, B-1
downloading RAF from a server, 2-6
duplicating ID resolutions, 6-8

E

elapsed CPU use, 7-23
enabling security, 4-2
enabling/disabling
  security, 4-7
  Source monitoring, 7-24
  Target security, 4-13
encryption
  definition in user profiles, 4-2
  of Peripheral Extension Module (PEM), 4-6
  passwords in RAF, 1-7, 4-14
  status change in Target user profile, 4-11
entries in script file, 4-16
environment
  customizing for RAF, 4-1
error messages for RAF, A-1
errors
  in data transmission, 7-6
  in PGS, D-6
  in RAF MP Bridge, D-7
  in RAF MP Service, D-8
  in RAF MP Terminal, D-8
  in RAF Source, D-2
  in RAF Source/Target user profiles, D-6
  in RAF Target, D-3
  in RS-232 Target Interface, D-5
establishing Target connections, 7-2
Ethernet, 3-7
event generation for InControl, 1-9
Event Manager system service, D-8
event message details, D-9
events
  activity, D-9
  class, D-9
  component, D-9
  details, D-1, D-9
  fields, D-9
  generation feature, 1-7

events (continued)
list of InControl events, D-1
Log.sys file, D-8
message documentation form, D-11
messages in log file, D-8
MP Bridge event message details, D-87
MP Service event message details, D-96
MP Terminal event message details, D-105
operator-generated flag, D-9
PGS event message details, D-80
RAF Source/Target user profile event message details, D-69
RAF Target event message details, D-30
RAF Bridge event message details, D-54
RAF RS-232 Target Interface event message details, D-60
run file name, D-9
subtopic, D-9
summary, D-1
topic, D-9
values for event fields, D-9
%V1, D-9
%V2, D-9
example MCR profile with fixed-length password, 4-9
exiting
from the Telephone Directory, 5-5
the Source user profile, 4-5
explanation of events, D-1

F

fatal errors in RAF operations, A-1
features
MCR redirection, 1-7
configurable keystroke transmission, 1-7
configurable video update time interval, 1-7
control/viewing notification, 1-6
customizeable configuration file, 1-6
event generation, 1-7
IPM, 1-7
LED and Beep redirection, 1-6
message posting, 1-6
monitor inhibitor, 1-6
monitoring detection, 1-6
mouse redirection, 1-6
online Help, 1-7
password, 1-7
password encryption, 1-7
platform options, 1-7
printer redirection, 1-7
record and playback, 1-6
remote debugging, 1-6
RS-232 dial-up connection, 1-7
scanning, 1-7
Source and Target dialog, 1-6
transferring files, 1-6
fields
for events, D-9
file name
examples for recording, 29
for record sessions, 7-27
for script file, 7-7
file transfer
status in user profiles, 4-2
to/from Target, 7-12

find Source user, 7-24
fixed-length password for MCR profile, 4-9
Floppy Copy command, 2-2
Floppy Installation command, 2-5
fonts in RAF Source, 7-7
form
  event message documentation, D-11
  to document RAF configuration, B-1
function keys
  for logon to Source user profile, 4-5
  for partition selection, 7-13
  for Target user profile, 4-11
  to select Target, 7-12
functionality of RAF, 1-2

G

general functionality of RAF, 1-2
general information on RAF, 1-1
generating events, 1-7
GPS, 7-25

H

hardware used with RAF, xix, 1-2
Help
  example screen, 7-2
  online, 7-1
Help bar, 30
hierarchy in security, 4-3
host connections, 3-8
How RAF works, 1-2

I

IBM connectivity, 3-10
ID of the Target, 6-6
ID resolution, 6-8
InControl
  event generation, 1-9
  list of events, D-1
  references, xx
information
  locating it in this guide, xvii
inhibiting monitoring, 1-6
install definition, 2-1
installation
  CTOS versions, 2-4
  determining which command to use, 2-2
  determining which components to install, 2-3
  Modem Service, 2-4
  preparing diskettes, 2-2
  procedures, 2-4
  RAF from a server, 2-6
installation and configuration terms, 2-1
installation diskette preparation, 2-2
Installation Manager command, 2-5
installing Event Manager system service, D-8
Interactive Performance Monitor (IPM), 1-7
  average CPU, 7-23
  elements of IPM monitor display, 7-23
  function keys, 7-24
  IPM Monitor screen, 7-22
  starting, 7-23
  update interval, 7-23
  view indicator, 7-23

interval of time for video update, 6-6, 7-25
introduction to RAF, 1-1
IPM, 1-7

K

keys
for IPM, 7-24
for playback, 7-31
keystroke transmission, 1-7

L

LAN, 1-1
LANs used with RAF, 3-2
LED redirection, 1-6
length of MP messages, 8-1
levels of access, 4-3
load definition, 2-1
loading
Device Service, 6-2
AA, CM, and CTOS Windows Services, 6-2
Local Event Management, 6-2
MCR Service, 6-2
Message Posting Bridge, 6-2
Modem Service, 6-2
onto XE520/XE530, 6-2
PGS, 6-2
RAF Target, 6-2
RS-232 Target Interface Service, 6-9
sequence, 6-2
Local Event Management
list of events, D-1
loading sequence with RAF software, 6-2
local fonts in RAF Source, 7-7
local system definition, 2-1
locating information in this guide, xvii
location of record file, 29
location of
Source/Target profile utilities, 4-1
user name and password for MCR, 4-2
log file size and name in user profile, 4-2, 4-13
Log on menu for RAF Source, 7-8
Log.sys file, D-8
logging maximum number of Targets, 6-4
logging on to RAF Source/RS-232 Source, 7-8
logon
function keys for Target user profile, 4-11
privileges, 4-3

M

Magnetic Card Reader (MCR)
character position on magnetic card, 4-9
example MCR profile, 4-8
procedures to create, 4-7
Profile form, 4-8
profile parameters, 4-8

magnetic card strip, 4-8
mainframe connectivity, 3-8
maximum characters in an MP message, 8-1
maximum number of concurrent sessions, 6-4
maximum number of Targets to log, 6-4
MCR profile, 4-2
  creating, 4-5
  fixed- and variable-length passwords, 4-9
MCR Service
  loading, 6-2
memory-loading sequence for RAF, 6-2
menu options for node selection, 7-10
Message Posting
  Bridge component, 1-9, 8-3
  capabilities, 8-1
  components, 8-3
  configuring BNet parameters
  creating messages, 8-5
  displaying messages, 8-11
  installing, 2-4
  loading, 8-4
  maximum characters in a message, 8-1
  maximum number of stored messages, 8-1
  Notification component, 8-3, 1-9
  overview, 8-1
  recalling messages, 8-7
  received messages and acknowledgements, 8-11
  saving, 8-6
  sending messages to all users, 8-10
Message Posting (continued)
  sending messages to Cluster LAN users, 8-8
  sending messages to other BNet nodes, 8-10
  sending messages via a distribution list, 8-11
  service, 8-3
  status codes, A-1
  supporting networks, 8-1
Message Posting Bridge, 1-9
  event summary table, D-7
  loading, 6-2
  summary of events, D-1
Message Posting Service
  event message details, D-87, D-96
  event summary table, D-8
  loading, 6-2
  summary of events, D-1
Message Posting Terminal
  event message details, D-105
  event summary table, D-8
  summary of events, D-1
messages
  creating for Message Posting, 8-5
  error, A-1
  events for InControl, 1-9
  for RAF Source errors, D-2
  for RAF Target errors, D-3
  list of events, D-1
  recalling, 8-7
  saving in Message Posting, 8-6
Modem Service
  access to WAN, 3-7
  actions with errors, 7-6
  included with RAF or BNet, 6-3
  loading, 6-2

Modem Service (continued)
network, 3-2
on Source and Target workstations, 3-11
references, xx
with RAF RS-232 Source software, 7-2
modes for monitoring, 7-14
modifying
a Source user profile, 4-5
a Target user profile, 4-13
a Telephone Directory, 5-2
user profile, 4-4
monitor inhibitor, 1-6
monitoring
defining the mode in script file, 4-16
detection, 1-6
modes, 7-14
over dial-up connection, 1-7
privileges for Source, 4-13
mouse redirection, 1-6, 6-3
Mouse Service
loading, 6-2

N

name of file for playback, 7-7
naming the record file, 7-27
networking terms, 3-1
networks
BNET, 3-2
BNET components, 3-5
BNet II, 3-2
BNet II components, 3-6
channel specification in script file, 4-16
cluster LAN, 1-2
component worksheet, B-1
components to use, 3-11
networks (continued)
configuring for RAF, 3-1
connecting RS-232 channels, C-1
CTOS cluster LAN, 3-2
dial-up, 3-10
definition, 3-1
documenting on component worksheet, 3-12
Ethernet, 3-7
IBM connectivity, 3-10
LAN definition, 1-1
LANs used with RAF, 3-2
mainframe connectivity, 3-8
modem service access to WAN, 3-7
OSI Transport layers, 3-7
OSI Session, 3-7
packet-switched, 1-1, 3-8
protocols, 1-3
RAF error messages, A-1
RS-232 dial-up connection, 1-7
SNA connectivity, 3-10
token ring, 3-7
typical channel specifications, C-2
WAN definition, 1-1
Wide Area Networks (WAN), 3-7
X.25, 3-8
node
menu options for selection, 7-10
selecting, 7-10
updating Target node screen, 7-10
node name for recording sessions, 7-27
node specification in script file, 4-16
:NoOfSendKeys: parameter, 2-7

notification
  message posting, 1-9
  of Source viewing or control, 1-6
  of system problems, D-1
:Notification: parameter, 2-8
:NotifyBlink: parameter, 2-8
null-modem cable, C-3

O

online Help, 1-7, 7-1
operational failures, A-1
operator-generated flag, D-9
options with platforms, 1-7
order for loading Message Posting components, 8-4
organization of this guide, xvi
OSI
  definition, 3-1
  networks on RAF, 3-7
  Session, 3-7
  Transport LAN definition, 3-2
  Transport layers, 3-7
output redirection from printer, 7-25
overview of RAF, 1-1
overview terms, 1-1

P

packet-switched network, 1-1, 3-8
parameters
  for *RAFConfig.sys* file, 2-7
  for script file, 4-16
  to load RAF Bridge, 6-4
  to load RAF Target, 6-6
  to start RAF Source/RS-232 Source, 7-7
  to start screen recording, 7-27
partition
  examining snapshots, 7-13
  starting a control session, 7-13
  selection, 7-12
  specification in script file, 4-16
partition viewing, 7-13
password
  change in Target user profile, 4-11
  default for Source user profile, 4-4
  definitions in user profiles, 4-2
  encryption in RAF, 4-14
PEM
  module for password encryption, 4-14
  references, xx
phone lines for voice processor module, C-2
planning for installation, 2-2
platform options, 1-7
playback
  feature, 1-6
  file name, 7-7
  Help bar, 30
  keys, 7-31
playing back sessions, 7-26
ports for communication, C-2
preinstallation planning, 2-2
preliminary steps before installing, 2-2
preliminary tasks before loading RAF, 6-1
printer redirection through script files, 4-16
printer redirection, 1-7, 6-7, 7-12
privileges
  for Source monitoring, 4-13
  on Source and Target, 4-3

problems documented in events, D-1
procedures to
  change administration name, password, or encryption, 4-5
  change video update time interval, 7-25
  complete dial-up menu, 7-9
  create a script file, 4-15
  create a Source user profile, 4-6
  create a Target user profile, 4-12
  create a Telephone Directory, 5-1
  create an MCR profile, 4-7
  create messages, 8-5
  create Target user profile, 4-10
  display messages, 8-11
  enable/disable security, 4-13
  install RAF, 2-4
  load RAF and related software, 6-11
  modify or delete a Source user profile, 4-7
  modify or delete a Target user profile, 4-13
  modify or delete a Telephone Directory, 5-2
  play back a recording session, 7-30
  recall messages, 8-7
  save messages, 8-6
  send messages to Cluster LAN users, 8-8
  send messages to other BNet nodes, 8-10
  send messages via distribution lists, 8-11
  sign on to profile utilities, 4-4
procedures to (continued)
  sign on to Target user profile, 4-10
  start a recording session, 7-26
  start RAF Source/RS-232 Source, 7-6
  stop a recording session, 29
  transfer files, 7-32
  use the script file, 4-17
process for establishing Target connections, 7-3
processors used with RAF, 1-2
profile
  form for MCR, 4-8
  Source user, 1-8
  Target user, 1-8
  utilities for Source and Target, 4-1
protocol definition, 3-2
protocols for LAN and WAN, 1-3

Q

Queue Manager, 7-25
Queue.index file, 7-25

R

RAF
  advice for problems, D-10
  basic BNet configuration, 1-4
  basic configuration, 1-2
  basic SuperGen Series configuration, 1-5
  Change Video Interval, 1-8
  components to use in networking, 3-11
  components, 1-8

RAF (continued)
configuring networks, 3-1
creating script files, 4-15
customizing the environment, 4-1
determining components to install, 2-3
downloading from a server, 2-6
encrypting passwords, 4-14
event summary, D-1
features, 1-6
how it works, 1-2
installing and configuring, 2-1
list of events, D-1
loading sequence, 6-2
managing a distributed environment, 7-1
monitoring workstations, 7-14
overview, 1-1
platform options, 1-7
preinstallation planning, 2-2
remedy for problems, D-10
security, 4-2
sending messages, 8-1
Source component, 1-8
Source user profile, 1-8
status codes, A-1
Target component, 1-8
Telephone Directory component, 1-8
transferring files, 1-6
with cluster LAN, 1-2
with Modem Service, 2-4
RAF Bridge, 1-2, 1-8
event message details, D-54
loading, 6-2
parameters to load, 6-4
procedures to load, 6-3
RAF Bridge (continued)
workstations that require Bridge, 6-3
summary of events, D-1
unloading, 6-4
RAF Change Video Interval, 1-8
RAF Performance Gathering Service (PGS)
event message details, D-80
event summary table, D-6
loading and unloading, 6-1
with IPM, 7-22
using, 7-1
RAF Query Video Interval, 1-8
RAF RS-232 Source
checking transmission for errors, 7-6
dial-up menu, 7-9
establishing connections, 7-2
local fonts, 7-7
logging on, 7-8
parameters, 7-7
playback file name, 7-7
starting, 7-6
telephone directory entry, 7-9
RAF RS-232 Target Interface
loading, 6-2
overview, 6-9
sessions supported, 6-9
software to install, 6-9
with Modem Service networks, 6-9
RAF screen recording, 1-8
RAF script, 1-8
RAF Source
event summary table, D-2
local fonts, 7-7
logging on, 7-8

RAF Source (continued)
parameters, 7-7
playback file name, 7-7
starting, 7-6
summary of events, D-1
RAF Source user profile
event message details, D-69
event summary table, D-6
summary of events, D-1
utility, 4-1
RAF Target
event message details, D-30
event summary table, D-3
loading, 6-2, 6-5
loading on an XE520/XE530, 6-5
parameters to load, 6-6
summary of events, D-1
unloading, 6-8
RAF Target user profile
event message details, D-69
event summary table, D-6
summary of events, D-1
utility, 4-1
RAF users
sections to read, xv
finding information in this guide, xvii
RAF workstation
establishing connections, 7-2
RAFTargetProfile.Sys file, 4-2
record and playback feature, 1-6, 6-7
recording screen, 1-8
recording session
file name, 7-27
file name examples, 7-29
location of file, 7-29
node name, 7-27
parameters to start recording, 7-27
recording session (continued)
partition name, 7-27
playback keys, 7-31
playing back, 7-30
playback Help bar, 30
sample configuration, 7-28
starting, 7-26
stoping, 7-29
workstation name, 7-27
redirection
Beep and LED keys, 1-6
MCR device, 1-7, 6-7
mouse, 1-6, 6-3
printer, 1-7, 6-7, 7-13, 7-25
printer through script files, 4-16
scroll frame, 6-7
references to other CTOS books, xx
related publications, xx
remedy for RAF problems, D-10
remote debugging, 7-14
report ID, D-9
resolving duplicate IDs, 6-8
RS-232
channel connections, C-1
dial-up feature, 1-7
node selection menu, 7-10
Source component, 1-8
Target component, 1-8
:RS232TimeOut: parameter, 2-7
run file name, D-9

S

sample configuration for RAF recording, 7-28
saving a message, 8-6

scan
  feature, 1-7
  mode of monitoring, 7-14
screen
  displaying Target on Source, 7-12
  recording (RAF component), 1-8
script file
  file name, 7-7
  parameters, 4-16
  using, 4-17
scroll frame redirection, 6-7
section contents, xvi
security
  for Target workstation, 4-13
  hierarchy, 4-3
  in RAF, 4-3
  with passwords, 1-7
selecting
  a node, 7-10
  a partition, 7-12
  a Target, 7-11
sending messages
  to all users, 8-10
  to Cluster LAN users, 8-8
  to other BNet nodes, 8-10
  via distribution lists, 8-11
sequence to establish Target connections, 7-3
sequence to load RAF software, 6-2
serial connectors, C-3
serial port specification in script file, 4-16
servers with RAF, xix
session definition, xix
sessions
  maximum number to log
setting privileges for Source monitoring, 4-13
Shared Resource Processor
  communication ports, C-2
  with RAF, 1-2
signing on to
  Source user profile, 4-4
  Target user profile utility, 4-10
SNA
  connectivity, 3-10
  definition, 3-2
  Transport, 3-10
Software Installation command, 2-5
software loading sequence, 6-2
Source and Target dialog, 1-6
Source definition, 2-1
Source Dial-Up menu, 5-4
Source monitoring
  enabling/disabling, 7-24
:SourceTimeOut: parameter, 2-7
Source user profile
  Administration form, 4-5
  changing user name, password, encryption, 4-5
  creating and modifying, 4-4
  creating, 4-5, 4-6
  default administrator name, 4-4
  defining security, 4-3
  definition, 4-1
  enabling/disabling security, 4-7
  exiting, 4-5
  information in profile, 4-2
  logon function keys, 4-5
  modifying or deleting, 4-7
  signing on to utility, 4-4

Source viewing notification, 1-6
Source workstation
  creating a Source user profile, 4-6
  definition, xix
  displaying Target CPU activity, 7-12
  displaying Target CPU status, 7-22
  entering Target debugger, 7-12
  error messages, A-1
  loading Message Posting, 8-4
  monitoring privileges, 4-13
  mouse redirection, 6-3
  network components to use, 3-11
  printer redirection from Target, 6-7
  record and playback, 6-7
  redirecting MCR to Target, 6-7
  remote debugging, 7-19
  starting a debugging session, 7-19
  scanning a Target, 7-20
  starting a scan mode, 7-20
  software loading sequence, 6-2
  specifying time for no activity, 7-7
  starting a control session, 7-17
  transferring files to/from Target, 7-13
  user profile overview, 4-1
  viewing a Target only, 6-6
specifications for typical RS-232 channels, C-1
status codes for RAF, A-1
structure of events, D-1
subsystem ID, D-9
subsystem string, D-9
subtopic, D-9
successive access to Targets, 7-12
summary of events for InControl, D-1
SuperGen Series
  basic configuration, 1-5
  workstations used with RAF, 1-2
system definition, 2-1
system problem notifications, D-1
system problems, A-1
systems management event messages, D-1
Systems Network Architecture (SNA), 3-2
:SzVidUpdateBuffer: parameter, 2-8

T

Target definition, 2-1
Target Selection screen, 7-11
Target user profile
  Administration form, 4-11
  changing administrator name, 4-11
  changing password, 4-11
  creating, 4-10, 4-12
  defining a log file, 4-13
  defining name and size of log file, 4-2
  defining Source user name and password, 4-2
  definition, 4-1
  encryption status change, 4-11
  information in profile, 4-2
  logon function keys, 4-11
  modifying/deleting, 4-13
  signing on, 4-10
  workstation identifier in profile name, 4-2

Target workstation
Action keys, 7-24
controlling, 7-12
CPU activity, 7-12
creating a Target user profile, 4-12
debugger, 7-12
defining a log file, 4-13
displaying CPU status, 7-22
displaying Target screen on Source, 7-12
duplicate Target ID resolution, 6-8
enabling/disabling security, 4-13
enabling/disabling Source monitoring, 7-24
error messages, A-1
finding Source user, 7-24
function keys to select, 7-12
ID, 6-6
loading Message Posting, 8-4
loading RAF Target, 6-5
monitoring detection, 1-6
mouse redirection, 6-3
network components to use, 3-11
parameters to load RAF Target, 6-6
printer redirection to Source, 6-7
privileges for Source monitoring, 4-13
RAFTargetProfile.Sys file, 4-2
redirecting MCR from Source, 6-7
scanning, 7-20
starting a scan mode, 7-20
selecting, 7-11
software loading sequence, 6-2
starting a control session, 7-17
transferring files to/from Source, 7-13
user profile overview, 4-1
Telephone Directory, 1-8
configuration, 5-1
creating, 5-1
entry in script file, 4-16
exiting, 5-5
modifying or deleting, 5-2
using, 5-4
terminology, xix
terms
used in installation and configuration, 2-1
used in overview, 1-1
used in networking, 3-1
time interval for video update, 1-7, 6-6
time specified for Source activity, 7-7
token ring, 3-7
topic, D-9
transferring files, 7-12, 7-32
transferring files to/from Targets, 7-13
transmission
asynchronous, 1-1
protocols, 1-3
transmitting keystrokes, 1-7
type of monitoring, 4-16
typical RS-232 channel specifications, C-1

U

Unisys mainframe connections, 3-8
unloading
Message Posting, 8-4
PGS, 6-11
RAF Bridge, 6-4

unloading (continued)
RAF Target, 6-8
RAF, 6-1
RS-232 Target Interface Service, 6-10
updating
partition list, 7-13
the Target node screen, 7-10
the Target selection list, 7-12
time interval for video, 1-7
user profile (Source), 1-8
users of this guide, xv
utilities
location of profile utility, 4-1
profile purpose, 4-1
RAF Query Target ID, 1-8
screen recording, 1-8
Source user profiles, 1-8
Source user profile overview, 4-1
Target user profiles, 1-8
Target user profile overview, 4-1

V

%V1, D-9
%V2, D-9
V Series mainframe connections, 3-8
values for event fields, D-9
variable-length password for MCR profile, 4-9
video update time interval, 1-7, 6-6, 7-12
view mode Action keys, 7-24
view mode of monitoring, 7-14
view notification, 6-6
viewing a Target only, 6-6
viewing partitions, 7-13

W

WAN, 1-1, 3-7
What RAF is, 1-1
wiring for null-modem cable, C-3
worksheet for documenting network, 3-12, B-1
workstation
definition of source, xix
definition of target, xix
workstation ID of the Target, 6-6
workstation identifier in Target user profile, 4-2
workstation specification in script file, 4-16
workstations
communication ports, C-2
managing with RAF, 7-1
monitoring, 7-14
used with RAF, 1-2
:WrapLogFileAllowed: parameter, 2-8
writing event messages to log file, D-8

X

X.25
definition, 3-2
networks, 3-8
XE Software Installation command, 2-5
XE520/XE530
communication ports, C-2
loading RAF Target, 6-5
with RAF RS-232 Target Interface, 6-9
with RAF software, 6-2

43935931-000

UNISYS

Product Information Announcement

● New Release ○ Revision ○ Update ○ Errata

Title:

CTOS® Remote Access Facility (RAF) R3.2 Installation, Administration, and Operations Guide

This Product Information Announcement (PIA) announces the release and availability of the *CTOS Remote Access Facility (RAF) R3.2 Installation, Administration, and Operations Guide*, part number 4393 5931-000.

This guide describes how to install and configure RAF R3.2. It also describes how to use RAF to manage distributed systems. RAF R3.2 also includes the accompanying *CTOS Remote Access Facility (RAF) Action Key Quick Reference* (document number 4393 5949-000).

To order additional copies of this document:

- United States customers can call Unisys direct at 1-800-448-1424
- All other customers, contact your Unisys Librarian
- Unisys personnel can use the Electronic Literature Ordering (ELO) system

We welcome all technical and documentation comments relative to this release.

Address your comments to: Unisys Corporation
Product Information
5155 Camino Ruiz
Camarillo, CA 93012

Call our feedback line at: 1-800-729-0451

Or, fax your comments to: (805) 389-4483

Unisys is a registered trademark of Unisys Corporation.
CTOS is a registered trademark of Convergent Technologies, a wholly owned subsidiary of Unisys.

Announcements only: BT188

Announcements and attachments: BT187, PR5, SA, SN, SU, SW

System: CTOS
Release: RAF R3.2.0 (September 1993)
Part Number: 4393 5931-000

UNISYS

Dear Customer,

This letter contains valuable inventory information to help you verify that you have received all product components that you ordered. If you have any questions about the completeness or condition of this package, please call your Unisys representative.

Thank you for choosing Unisys.

System:	**CTOS®**
Product Name:	**CTOS Remote Access Facility (RAF)**
Date:	**September 1993**
Release Level:	**R3.2.0**
Media:	**3-1/2 inch diskettes**
Product Styles:	**MB25-RAF, XB25-RAF, NP25-RAF, UP25-RAF**
Workstation/Server Type:	**B24, B26, B27, B28, B38, B39, SG1000, SG2000, SG3000, SG5000, XE-520, XE-530**

The following product components table contains:

- Name and part number for each product component
- Checklist boxes you can use to confirm that the shipment is complete

Information on the features of CTOS Remote Access Facility (RAF) R3.2.0 can be found in the *CTOS Remote Access Facility R3.2.0 Software Release Announcement.*

Unisys is a registered trademark of Unisys Corporation.

CTOS is a registered trademark of Convergent Technologies Inc., a wholly owned subsidiary of Unisys Corporation.

Note: *Part numbers are for identification purposes only. Refer to the CTOS Remote Access Facility (RAF) R3.2.0 Software Release Announcement (SRA) for ordering information.*

Product Components Checklist

Part Description	Part Number	✔
Documentation		
CTOS Remote Access Facility (RAF) R3.2.0 Cover Letter	4393 3233-001	✔
CTOS Remote Access Facility (RAF) R3.2.0 Software Release Announcement	4393 3217-001	❑
CTOS Remote Access Facility (RAF) R3.2 Installation, Administration, and Operations Guide	4393 5931-000	❑
CTOS Remote Access Facility (RAF) R3.2 Action Key Quick Reference	4393 5949-000	❑
CTOS Modem Service 5.02.05 Software Release Announcement	4371 5184-000	❑
CTOS Modem Service 5.1 Operations and Programming Guide	3912 6107-000	❑
2 3/4-inch binders with slipcase	—	❑
Software		
CTOS Remote Access Facility (RAF) R3.2.0 2 diskettes, 3-1/2 inch, for the following style:		
B25-RAF	3765 4175-000	❑
CTOS Modem Service 5.02.05 1 diskette, 3-1/2 inch, for the following style:		
MB25-MDM	4371 5150-000	❑
1 vinyl diskette holder	—	❑

43933233-001

UNISYS

Software Release Announcement

CTOS® Remote Access Facility (RAF) R3.2.0

product acronyms:

RAF

product aliases:

MB25-RAF
XB25-RAF
NP25-RAF
UP25-RAF
ML25-RAF
UL25-RAF

You can order additional copies of this document through your branch representative or from Unisys Corporation, Corporate Software and Publications Operations, 13250 Haggerty Road North, Plymouth, Michigan 48170.

Distribution lists (UML):
PR5, SA, SN, SU, SW, BT187, BT188

System: CTOS
Release R3.2.0
September 1993
Part Number: 4393 3217-001

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product and related material disclosed herein are only furnished pursuant and subject to the terms and conditions of a duly executed Program Product License or Agreement to purchase or lease equipment. The only warranties made by Unisys, if any, with respect to the products described in this document are set forth in such License or Agreement. Unisys cannot accept any financial or other responsibility that may be the result of your use of the information or software material, including direct, indirect, special or consequential damages.

You should be careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used.

The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Correspondence regarding this publication should be forwarded to Unisys Corporation by addressing remarks to Product Information, 5155 Camino Ruiz, Camarillo, CA 93012 U.S.A.

The names, places, and/or events used in this publication are not intended to correspond to any individual, group, or association existing, living, or otherwise. Any similarity or likeness of the names, places, and/or events with the names of any individual, living or otherwise, or that of any group or association is purely coincidental and unintentional.

Copyright © 1993 Unisys Corporation, All rights reserved.

Context Manager, Shared Resource Processor, and SRP are registered trademarks of Convergent Technologies Inc., a wholly owned subsidiary of Unisys Corporation.

CTOS and SuperGen are trademarks of Convergent Technologies, Inc.

MAPPER, OFIS, and Unisys are registered trademarks of Unisys Corporation.

CUSTOMCARE and MAPPER are registered service marks of Unisys Corporation.

CTOS InControl and BTOS are trademarks of Unisys Corporation.

Presentation Manager is a trademark of International Business Machines Corporation.

Contents

Section 1 General Description 1

Introduction 1
Product Description 2
CTOS InControl Family of Products 2
CTOS Remote Access Facility R3.2.0 2
How to Order CTOS RAF R3.2.0 3

Section 2 Release Functionality 5

Enhancements 5
Supported on SuperGen Series 1000 5
MCR Service 5
RAF Bridge Supports 128 Targets 5
RAF Source Can Use NetCfg.sys 5

Section 3 Product Interdependencies 7

Interdependent Software 8
Interdependent Hardware 10
Workstations and Processors 10
Monitors 10
Keyboards and Pointing Devices 11
Disk Drives 11
Media Sizing 12
Random-Access Memory (RAM) Sizing 14

Section 4 Migration Requirements 15

CTOS RAF 3.0 or 3.1 to R3.2.0 Migration Tasks 15
CTOS RAF 2.1 to R3.2.0 Migration Tasks 15
Interoperating with Earlier Versions of RAF 16
Upgrade Assistance 16

Section 5 Product Corrections 17

Message Posting to ALL Users 17
Using Screen Setup in Control Sessions 17
ACTION+FINISH during Chit-Chat 17
Target Keyboard Is Locked Out after Logoff in Control Session 17
Transferring Files from Remote Site to XE-530 18
Installing RAF Target with K4 Keyboard 18
RAF RS-232 Target Abnormal Termination Handling 18

Section 6 Restrictions and Known Limitations 19

New Items 19
Existing Items 19
Font Incompatibilities 19
LED Mapping to the SuperGen Series 3000 19
Video Attribute Mapping to the SuperGen Series 3000 . 20
Color Palette Mapping 20
Using Custom Fonts 20
Remote Debugging Limitations 20
RS-232 Source Limitations 21
RAF Keyboard Limitations 21
Notification after Abnormal Termination of Session ... 21
Message Posting Limitations 21
Screen Recording Limitation 21
RAF Screen Setup Limitation 22
Chit-Chat 22
Modem Profile 22
B24 Workstation Limitations 23
Performance Gathering System Limitations 23
System Hang While Restarting Software Distribution .. 23
System Hang after Controlling Display Manager 23

Section 7 Support 25

Support Discontinuance 25

Section 8 Customer Product Information 27

Section 9 List of Files on the Product Media 29

Files on 3½-inch Diskettes 29
Files on 5¼-inch Diskettes 31

Section 10 Ordering Procedure 33

Part Numbers 33
CTOS RAF R3.2.0 Components You Can Order 34

Section 1
General Description

This section contains:

- An introduction to the Software Release Announcement (SRA)
- A concise description of CTOS Remote Access Facility R3.2.0 software, including major options and important new or existing features, and information on related families of products
- CTOS Remote Access Facility R3.2.0 product style names and available distribution media you can order

Introduction

Unisys publishes Software Release Announcements (SRAs) to announce the release of a new product. An SRA:

- Provides you with technical details and ordering information on the new product
- Prescribes interdependency and migration considerations
- Complements marketing, sales, and other customer product information
- Lists additional sources of information

You can order extra copies of an SRA. For more information, see Section 10, Ordering Procedure, or contact your Unisys representative.

Product Description

CTOS Remote Access Facility is part of the CTOS InControl family of cooperating products and services.

CTOS InControl Family of Products

The CTOS InControl family of products provides an integrated set of services for managing distributed CTOS hardware and software over a communications network. Other CTOS InControl products include CTOS Local Event Management (LEM), CTOS Integrated Event Monitor (IEM), and CTOS Software Distribution (SWD).

CTOS Remote Access Facility R3.2.0

CTOS Remote Access Facility R3.2.0 (RAF) is a set of software products that allows one workstation to view or control another workstation (or memory partition on a workstation). These workstations are connected over a BTOS BNET, CTOS BNet II, or CTOS Cluster LAN, or over an asynchronous dial-up network using CTOS Modem Service.

CTOS RAF provides both user-access security and hierarchical security for its features.

The CTOS RAF software provides a user interface for performing the following tasks:

- Selecting nodes, workstations, and partitions to view or control
- Selecting global network configuration file names
- Creating user profiles for specifying user access to RAF Source and Target workstations
- Defining entries in a telephone directory for asynchronous dial-up access
- Creating script files for automating RAF operations
- Recording and playing back Target workstation activities
- Monitoring Target workstation CPU utilization

The CTOS RAF R3.2.0 package includes the CTOS Modem Service product (also available separately). For information about installing and operating the Modem Service, refer to the *CTOS Modem Service 5.02.05 Software Release Announcement* and the *CTOS Modem Service Operations and Programming Guide*.

How to Order CTOS RAF R3.2.0

Section 10 contains complete ordering information.

Note: *CTOS RAF R3.2.0 is available on both 3 1/2-inch and 5 1/4-inch media.*

Section 2
Release Functionality

This section describes the new and enhanced features of CTOS Remote Access Facility R3.2.0.

Enhancements

New enhancements provided in CTOS RAF R3.2.0 are described below.

Supported on SuperGen Series 1000

CTOS RAF R3.2.0 is now supported on the SuperGen 1000 series of laptop workstations for RAF Source only.

MCR Service

CTOS RAF R3.2.0 now supports MCR redirection of the EF 4552-DL2 MCR using the CTOS MCR Service without CTOS Device Service. Previous releases required both services for all MCR devices.

RAF Bridge Supports 128 Targets

RAF Bridge now supports up to 128 Targets. The previous limit was 40.

RAF Source Can Use NetCfg.sys

If the BNet Naming Service is not available, RAF Source now displays the node names in *NetCfg.sys*. (This feature was present in RAF 3.0.1, but removed in 3.1.)

Section 3
Product Interdependencies

This section contains:

- Information on interdependent software releases and hardware you need to use with the various functional components in the CTOS RAF R3.2.0 package
- Information on the supported software release levels of all required products
- Random-access memory (RAM) and media sizing requirements

You can use the information in this section to configure your system. A suggested configuration for minimal input/output functionality includes:

- Your CTOS hardware, including a hard disk, networking modules, and modems
- Your CTOS operating system
- Your networking software

Interdependent Software

The following tables describe the interdependent software releases you need to use the CTOS RAF R3.2.0 package, the nature of the interdependencies, and lists the style names and release levels (for ordering purposes). For products that have had recent releases, the tables may also include the previous release level.

Older releases of interdependent software may work with CTOS RAF R3.2.0, but Unisys may not fully support them. If you require a correction to an older release, Unisys may ask you to upgrade to a newer release.

As new releases become available, Unisys may no longer offer certain ordering and support services for older releases. Review the applicable Software Release Announcement (SRA) for future compatibility and service information. See Section 10, Ordering Procedure, for part number information to order an SRA.

Operating Systems

Software Description	Style ID	Release
BTOS II	(see Notes)	3.2.0 or greater
CTOS I and II	(see Notes)	3.3.1 or greater
CTOS III	(see Notes)	1.1 or greater
CTOS/XE	XE530-MOS	3.0 or greater

You also need the Standard Software that Unisys specifies for your operating system.

Other Interdependent Software

Software Description	Style ID	Release
Networking Software:		
CTOS BNet II	B25-BNT	2.1.0 for BTOS II, CTOS I, and CTOS II prior to 3.4
CTOS BNet II	B25-BNT	3.1.0 for CTOS II 3.4 and CTOS III
CTOS Modem Service	B25-MDM	(see Notes)
Other Software:		
CTOS Context/Window Manager	B25-CM6	use the release that your operating system supports
CTOS InControl Local Event Management (optional for event monitoring)	B25-LEM	2.0 or greater
CTOS Peripheral Extension Module (PEM) Server (optional for RAF password encryption)	B25-PEM	6.1.0 or greater
CTOS II Device Server (optional for MCR redirection)	B25-DEV	6.1.0 or greater

Notes: *Style IDs vary according to CPU type (B24 through B39, SuperGen Series) and Operating System type (Server, Cluster, or Stand-alone workstations).*

For more information on equipment configurations, software, and Style IDs, contact your Unisys representative.

Additional information is also available in the Software Release Announcements associated with the various products.

CTOS RAF R3.2.0 includes CTOS Modem Service 5.02.05. Use this Modem Service if you do not use BNet. If you use BNet, use the Modem Service provided with the BNet package.

Interdependent Hardware

This section provides information on hardware products you can use with CTOS RAF R3.2.0. Hardware includes workstations, processors, monitors, keyboards, networking devices, and magnetic card readers.

Workstations and Processors

CTOS RAF R3.2.0 requires one of the following workstations:

B24	SuperGen Series 1000 (RAF Source only)
B26	SuperGen Series 2000
B27	SuperGen Series 3000
B28	SuperGen Series 5000
B38	
B39	

You can load and execute RAF Bridge or the Message Posting Bridge on any XE processor board. You can load RAF RS-232 Target Interface on an XE Cluster Processor (CP) board or General Processor (GP) board with RS-232 connections. You should load both Modem Service and RAF RS-232 Target Interface on the same XE processor board.

You cannot load or execute RAF Source, RAF Target, Message Posting Service, or Message Posting Notification on an XE Shared Resource Processor.

Monitors

CTOS RAF R3.2.0 requires a monitor. It does not require a graphics device. RAF displays in character mode on all text and graphic systems that your operating system supports. RAF cannot display graphics written directly to the graphics bit map.

Keyboards and Pointing Devices

You can use CTOS RAF R3.2.0 with the following keyboards:

B25-K1	SG101-K
B25-K2	SG102-K
B25-K3	B25-K4 (Limited support - See Section 6)
B25-K5	

CTOS RAF R3.2.0 allows mouse redirection in character mode. RAF does not support mouse redirection for graphic applications. You can use the following mice, which require the Mouse Service included with your Standard Software:

B25-MOU	B25-MO3
SG100-U	SG101-U

Disk Drives

CTOS RAF R3.2.0 requires a hard disk drive and either a 3-1/2-inch or 5-1/4-inch drive for software installation.

Media Sizing

The following table lists approximate media sizing considerations for all required and optional installation files.

Description	Sectors
For RAF Source installation:	
RAFSource.run	539
RAFProfile.run	195
RAFConfig.sys	6
RAFSourceProfile.sys	3
IPM.font	16
B27IPM.font	16
AGPIPM.font	18
SG3IPM.font	18
Total RAF Source required disk space	811
For RAF Target Installation:	
RAFBridge.Run	55
RAFDeinstallBridge.Run	22
RAFTarget.Run	288
RAFDeinstallTarget.Run	14
RS232Target.Run	179
DeinstallRS232Target.Run	18
RAFProfile.Run	195
RAFTargetProfile.Sys	3
RAFConfig.sys	6
RAFQueryChangeTime.Run	84
PGS.Run	58
RAFLog.Run	12
DeinstallPGS.Run	9
Total RAF Target required disk space	935

continued

Media Sizing (continued)

Description	Sectors
For RAF Message Posting installation:	
MPBrdg.Run	89
MPSrvr.Run	92
MPTerm.Run	232
DeinstMPSrvr.Run	57
DeinstMPBrdg.Run	41
MPBrdg.Msg	6
MPSrvr.Msg	6
MPTerm.Msg	28
Total RAF Message Posting required disk space	551

Random-Access Memory (RAM) Sizing

As a guideline, the following table shows the RAM considerations you can use as a typical memory requirement. Your particular use will determine your exact RAM needs.

Using this table, you can also identify the mode of memory each program uses. Each program will use all available memory in its partition, up to the maximum.

Description	Memory Mode	K Bytes RAM
System services:		
RAF Bridge	Protected	25
RAF Target	GDT Protected	189 + 16 for each additional Source
RAF RS-232 Target Interface	Protected	106
RAF PGS	Protected	43 + 3 for each additional Source
Message Posting Bridge	Protected	57
Message Posting Service	Protected	42
User applications:		
RAF User Profile Utility	Protected	334
RAF Source (standard or RS-232)	Protected	487
Message Posting Notification	Protected	124

Section 4
Migration Requirements

This section describes the tasks required to migrate from prior releases of CTOS RAF.

CTOS RAF 3.0 or 3.1 to R3.2.0 Migration Tasks

If you are upgrading from RAF 3.0, you must recreate any script files that you are using. Script files are not compatible between the two versions. Script files created with RAF 3.0.2 or later are compatible.

If you are upgrading from RAF 3.0 or 3.1 to RAF R3.2, save the default profiles *RAFSourceProfile.Sys* and *RAFTargetProfile.Sys* files prior to installing RAF R3.2.0, and restore them afterwards.

CTOS RAF 2.1 to R3.2.0 Migration Tasks

RAF R3.2.0 user profiles are not compatible with RAF 2.1 or earlier versions. The R3.2.0 installation process overwrites the default profiles *RAFSourceProfile.Sys* and *RAFTargetProfile.Sys*. If you are upgrading from RAF 2.1, you must recreate your Source and Target user profiles. Use the following procedure when upgrading from RAF 2.1 or earlier:

1. Record all information from existing RAF profiles prior to installing RAF R3.2.0 software.
2. Install RAF R3.2.0.
3. Use the RAF Source User Profile and RAF Target User Profile utilities to recreate the user profiles.

Interoperating with Earlier Versions of RAF

RAF R3.2.0 can interoperate fully with RAF 3.0.1 or higher. It can interoperate with RAF 2.1.0 or higher Targets only.

RAF R3.2.0 does not coexist with any previous versions of RAF on the same node. Upgrade all workstations on a given node to RAF R3.2.0 at the same time.

Some of the command names of RAF 2.1 were changed in RAF 3.0 and above. The RAF R3.2.0 installation process removes the old command names from the command file.

Upgrade Assistance

For details on available upgrade assistance services and details on Unisys support eligibility, contact your Unisys representative or reseller.

Section 5
Product Corrections

This section describes corrections to certain restrictions, limitations, and operational conditions found in the releases of CTOS RAF preceding R3.2.0. Corrections are described relative to the operating environment, including a brief description of the original symptoms, if necessary.

Message Posting to ALL Users

The Message Posting function for sending messages to ALL users (local and remote nodes) now functions correctly. In previous releases, it sent them to users on the local cluster only.

Using Screen Setup in Control Sessions

The SuperGen Series 2000 screen now displays properly when you use the **Screen Setup** command to set narrow characters at the Target workstation.

ACTION+FINISH during Chit-Chat

Pressing **ACTION+FINISH** during a Chit-Chat session on CTOS III disables the Target keyboard until either the Target or Source user terminates the Chit-Chat session.

Target Keyboard Is Locked Out after Logoff in Control Session

The Target keyboard is now properly locked out after logoff during a Control session. In the prior releases, the Target user had full control until the Source user pressed a key. This problem occurred with the CTOS-II regular signon screen only.

Transferring Files from Remote Site to XE-530

RAF now properly transfers files from a remote B20 site to an XE without generating errors 10673 and 10560 and without clearing the RAF RS-232 Target partition.

Installing RAF Target with K4 Keyboard

RAF Target now installs properly on a workstation that has a K4 keyboard.

RAF RS-232 Target Abnormal Termination Handling

RAF RS-232 Target now handles abnormal terminations properly. In prior releases, an abnormal termination at the RS-232 Target caused the Source to hang.

Section 6
Restrictions and Known Limitations

The following restrictions and known limitations exist for CTOS RAF R3.2.0.

New Items

None.

Existing Items

The following restrictions and known limitations exist from prior releases of CTOS RAF. Except where noted, these items are a permanent part of the CTOS RAF product design.

Font Incompatibilities

When the Target loads a custom font, RAF Source attempts to load the same font if the video monitors are compatible. However, the SuperGen Series 3000 with standard VGA is NOT compatible with any of the other video monitors in the product line. Thus if the Target loads a custom font, RAF Source uses its current font. The displays will, therefore, differ.

LED Mapping to the SuperGen Series 3000

If the Target is a SuperGen 3000 and the Source is not, the LEDs on **F9** and **F10** of the Source's keyboard reflect the states of the Target's **SCROLL LOCK** and **NUM LOCK** LEDs, respectively.

If the Source is a SuperGen 3000, RAF does not alter the **SCROLL LOCK** and **NUM LOCK** LEDs to reflect the Target's LEDs, since the state of these LEDs affects the local keyboard operation.

The **SHIFT LOCK** LED on RAF Source always reflects the **SHIFT LOCK** LED state of the Target.

Video Attribute Mapping to the SuperGen Series 3000

The SuperGen Series 3000 with standard VGA does not support some video attributes (underline, bold, struck-through), and supports others (blinking, reverse video) in a different manner than the other video monitors in the product line. RAF attempts to determine the corresponding attributes. In some cases there are ambiguities, so some attributes may not be reflected correctly, or at all, or characters with certain attributes may be displayed in a different color.

Color Palette Mapping

Changes in color palette are not maintained across RAF. Therefore, the Source may display in different colors than the Target, even though both are equipped with color monitors of similar capabilities.

Using Custom Fonts

When the Target application is using a custom font, other RAF functions such as Chit-Chat and video monitoring notification use the same custom font.

Remote Debugging Limitations

On workstations running with BTOS II 3.2 or lower, RAF Target must be loaded before you invoke the debugger. Otherwise, the cursor will not show the correct location during remote debugging and the performance will be slightly degraded. Unloading RAF Target and invoking the debugger after a Debugging session may cause a crash. These problems do not occur on workstations running CTOS 3.3.1 or higher operating system.

If performing Remote Debugging in high resolution mode, the debugger display on the Source may become skewed. To fix the problem use the **Screen Setup** command to set the resolution of the Target Monitor to a lower resolution. If this does not work (some VGA systems), you must use a high resolution display on the Source workstation.

RS-232 Source Limitations

Running RS-232 Source on slow processors may result in status code 2346 (Receive overrun). If this happens, either load Modem Service on your own workstation (if you are using a cluster workstation) or use a lower baud rate.

RAF Keyboard Limitations

If the RAF keyboard buffer becomes full, excess keystrokes are discarded.

RAF provides limited support for the K4 keyboard. If K4 keyboards are used, they must be connected to both the Source and Target workstations and use the same *K4Sys.keys* files. Also, certain **ACTION** key combinations do not work when using the K4 keyboard.

RAF does not support applications that load their own keyboard tables. These applications include, but are not limited to, XVT and Presentation Manager.

The keyboard attached to the Target workstation should not be changed after loading RAF Target. Also, the keyboard attached to the Source workstation should not be changed during a control session.

Notification after Abnormal Termination of Session

If a View/Control session terminates abnormally (for example, the partition being viewed is swapped), the notification character may show, even though the View/Control session has terminated, until the screen is refreshed.

Message Posting Limitations

Messages sent to a cluster LAN for user X will be distributed to all users that are signed on to that cluster using the name X.

ACTION+D to display a message does not work on high resolution VGA systems in 38 line mode.

Screen Recording Limitation

This option does not display properly when the recording session is performed on a workstation that has the screen set to small characters (**Screen Setup,** *[Large character]* = **No**).

RAF Screen Setup Limitation

If the screen resolution changes during a RAF session, the screen display may become corrupted. To correct this problem, press **ACTION+CANCEL** followed by the **Cntrl** or **View** function key.

Chit-Chat

Chit-Chat is not allowed on AGP graphics systems when Context Manager is running.

Chit-Chat windows do not display on a Target workstation using a GC-004 monitor running in 38 line mode. You should use the Screen Setup command to reduce the number of lines of display before using Chit-Chat.

Modem Profile

If, when using Modem Service, the calling side appears to go on line, then drops immediately, try adding a delay to the *Sys.modems* file at the end of the **[Make_A_Call]** script for the modem involved. Typically, these scripts end with statements similar to the following:

```
:JumpIfCompareNotEqual:1
:OnLine:
:Finish:
```

Change this to

```
:JumpIfCompareNotEqual:2
:Delay:2
:OnLine:
:Finish:
```

You can experiment with varying the delay. The `JumpIfCompare` statement specifies the number of steps to skip if the condition is met, and thus needs to be increased to include the `delay` step added here.

B24 Workstation Limitations

The following RAF functions are not available on B24 workstations:

- Chit-Chat
- Monitoring detections
- Remote debugging
- Message posting
- Target CPU utilization display from RAF Source

Performance Gathering System Limitations

Unloading PGS while CPU utilization is being viewed may crash the Target workstation.

PGS works only in low resolution.

System Hang while Restarting Software Distribution

A RAF Target workstation may hang while restarting an aborted software distribution in the following combination of conditions:

- You are using CTOS InControl Software Distribution 2.2.
- The Target is running Context Manager.
- The Target user has dead mail.
- The Target node is in a view session.

If this situation occurs, reboot the Target workstation.

System Hang after Controlling Display Manager

A RAF Target workstation running Display Manager in a control session may hang if the Target user moves the mouse immediately prior to the end of the Control session.

To prevent this condition, ensure that the Source user makes the last mouse move before termination of the control session.

Section 7
Support

This section provides support categories and warranties information. It also provides information about any discontinuance of support for previous release levels (or features in those releases). Unisys may also provide you with information about support discontinuance in a Discontinuance Announcement.

The CTOS RAF R3.2.0 software is in Support Category 1 and Warranty Class 1. It is fully supported and enhanced, and it is warranted for 90 days to conform to Unisys published specifications.

Support Type	Statement
Support Category 1	fully supported and enhanced
Support Category 2	supported only, with no enhancements
Support Category 3	neither supported nor enhanced

Warranty Type	Statement
Warranty Class 1	warranted for 90 days to conform to Unisys published specifications
Warranty Class 2	not warranted and is provided "as is"

Support Discontinuance

Effective with the release of CTOS RAF R3.2.0, update maintenance support for all releases of RAF prior to 3.0.1 is discontinued. If you are currently using such a release level, you should consider migrating to release level R3.2.0 at the earliest opportunity. If you require a correction to a prior release level, Unisys may ask you to upgrade to release R3.2.0.

Section 8
Customer Product Information

Unisys packages product information into Libraries or Literature Sets for each product. Also, for your convenience, Unisys offers various ways to reorder product information to fit your needs.

- Library: Customers who wish to purchase the entire suite of books, including binders and slipcases, may do so by ordering the Library part number.
- Literature Set: Customers who wish to purchase individual books with binders and slipcases may do so by ordering the Literature Set part number.
- Individual books: Customers who wish to purchase individual books without binders and slipcases may do so by ordering the book part number.

See Section 10, Ordering Procedure, for part number information. Unisys includes all applicable errata and updates with each part number. Updates contain any preceding errata.

As release levels higher than those listed become available, review the applicable SRA for compatibility information.

Section 9
List of Files on the Product Media

This section describes the software distribution media. It organizes this information by available media. The CTOS RAF R3.2.0 package contains either two 3-1/2 inch diskettes or three 5-1/4 inch diskettes.

The following tables list the volume, directory, and file names on each type media.

Files on 3½-inch Diskettes

Location	File names	
B25RAF-1		
<Sys>:	BadBlk.sys	BootRecord.sys
	CrashDump.sys	DirectD.Cmds
	FdSys.version	Fileheaders.sys
	Install.Cmds	Install.ctrl
	Install.jcl	Log.sys
	MessageP.Cmds	Mfd.sys
	ProfileU.cmds	SMS.Registration
	SysImage.sys	
<Unisys>:	Request.RAF.sys	RafSourceProfile.sys
	MPBrdg.run	DeInstMPBrdg.run
	MPSrvr.run	DeInstMPSrvr.run
	MPBrdg.Msg	MPRqst.sys
	MPSrvr.Msg	MPTerm.Msg
	MPTerm.run	RAFConfig.sys
	RAFProfile.run	RAFSource.run
	SG3IPM.font	AGPIPM.font
	B27IPM.font	IPM.font

Location	File names	
B25RAF-2		
<Sys>:	BadBlk.sys	BootRecord.sys
	BridgeU.cmds	CrashDump.sys
	DirectD.Cmds	FdSys.version
	Fileheaders.sys	Install.Cmds
	Install.ctrl	Install.jcl
	Log.sys	MessageP.Cmds
	Mfd.sys	ProfileU.cmds
	SMS.Registration	SysImage.sys
<Unisys>:	RAFBridge.run	RAFDeInstallBridge.run
	RAFTarget.run	RAFDeInstallTarget.run
	RS232Target.run	DeInstallRS232Target.run
	RAFConfig.sys	RAFQueryChangeTime.run
	RAFProfile.run	RafTargetProfile.sys
	MPBrdg.run	DeInstMPBrdg.run
	MPSrvr.run	DeInstMPSrvr.run
	MPTerm.Msg	MPTerm.run
	Request.RAF.sys	MPBrdg.Msg
	MPRqst.sys	MPSrvr.Msg
	PGS.run	DeinstallPGS.run
	RAFLog.run	
<ECD>:	MpBrdg.ecd	MpSrvr.ecd
	MpTerm.ecd	pgs.ecd
	rafbridge.ecd	RafProfile.ecd
	rafsource.ecd	raftarget.ecd
	rs232target.ecd	

Files on 5¼-inch Diskettes

Location	File names	
B25RAF-1		
<Sys>:	BadBlk.sys	CrashDump.sys
	DirectD.Cmds	FdSys.version
	Fileheaders.sys	Install.Cmds
	Install.ctrl	Install.jcl
	Install.sub	InstallD.sub
	InstallM.sub	InstallNP.sub
	InstallP.sub	InstallRAF.sub
	InstallU.sub	Log.sys
	MergeRqs.sub	Mfd.sys
	ProfileU.cmds	SMS.Registration
	SysImage.sys	XeInstall.sub
<Unisys>:	AGPIPM.font	B27IPM.font
	IPM.font	RAFConfig.sys
	RAFProfile.run	RAFSource.run
	Request.RAF.sys	SG3IPM.font
	RafSourceProfile.sys	
B25RAF-2		
<Sys>:	BadBlk.sys	BridgeU.cmds
	CrashDump.sys	DirectD.Cmds
	FdSys.version	Fileheaders.sys
	Install.Cmds	Install.ctrl
	Install.jcl	Install.sub
	InstallB.SUB	InstallD.sub
	InstallM.sub	InstallNP.sub
	InstallP.sub	InstallRAF.sub
	InstallU.sub	Log.sys
	MergeRqs.sub	Mfd.sys
	SMS.Registration	SysImage.sys
	XeInstall.sub	
<Unisys>:	PGS.run	DeinstallPGS.run
	RAFBridge.run	RAFDeInstallBridge.run
	RAFTarget.run	RAFDeInstallTarget.run
	RS232Target.run	DeInstallRS232Target.run
	RAFConfig.sys	Request.RAF.sys

Location	File names	
B25RAF-3		
<Sys>:	BadBlk.sys	CrashDump.sys
	FdSys.version	Fileheaders.sys
	Log.sys	MessageP.Cmds
	Mfd.sys	ProfileU.cmds
	SMS.Registration	SysImage.sys
<Unisys>:	RAFProfile.run	RAFQueryChangeTime.run
	MPBrdg.run	DeInstMPBrdg.run
	MPSrvr.run	DeInstMPSrvr.run
	MPBrdg.Msg	MPRqst.sys
	MPSrvr.Msg	MPTerm.Msg
	MPTerm.run	RAFLog.run
	RafTargetProfile.sys	
<ECD>:	MpBrdg.ecd	MpSrvr.ecd
	MpTerm.ecd	pgs.ecd
	rafbridge.ecd	RafProfile.ecd
	rafsource.ecd	raftarget.ecd
	rs232target.ecd	

Section 10
Ordering Procedure

This section provides software and product information part numbers and release levels.

The update service request (USR) letter that is included with this document describes the ordering procedure. The USR letter includes:

- Available product style numbers
- Your order number
- Toll-free phone number for calling in orders
- Address for mailing in orders

For further assistance call your Unisys representative. United States customers call Unisys Direct at 1-800-448-1424.

Part Numbers

You can use the Style IDs or Part Numbers in the following tables to order CTOS RAF R3.2.0 components, including:

- Software media (distribution diskettes)
- The SRA (this document)
- Product Information

CTOS RAF R3.2.0 Components You Can Order

Note: *The following Style IDs include the Modem Service software, which has its own SRA.*

Style ID	CTOS Remote Access Facility (RAF) Software Media Description	Release Level
MB25-RAF	3 1/2-inch diskettes or 5 1/4-inch diskettes	R3.2.0
XB25-RAF	3 1/2-inch diskettes or 5 1/4-inch diskettes	R3.2.0
NP25-RAF	3 1/2-inch diskettes or 5 1/4-inch diskettes New Package License	R3.2.0
UP25-RAF	3 1/2-inch diskettes or 5 1/4-inch diskettes Upgrade Package License	R3.2.0
ML25-RAF	New Package License only	R3.2.0
UL25-RAF	Upgrade Package License only	R3.2.0

Documentation Description	Release Level	Part Number
CTOS Remote Access Facility (RAF) Software Release Announcement (SRA)	R3.2.0	4393 3217-001
CTOS Remote Access Facility (RAF) Document Library	R3.2	4164 1291-001
The library consists of:		
CTOS Remote Access Facility (RAF) Installation, Administration, and Operations Guide	R3.2	
CTOS Remote Access Facility (RAF) Action Key Quick Reference	R3.2	
3/4-inch binder and slipcase		
CTOS Modem Service Operations and Programming Guide	5.1	
3/4-inch binder and slipcase		

Documentation Description	Release Level	Part Number
CTOS Remote Access Facility (RAF) Installation, Administration, and Operations Guide Literature Set	R3.2	4393 5956-000
Which includes:		
CTOS Remote Access Facility (RAF) Installation, Administration, and Operations Guide	R3.2	
3/4-inch binder and slipcase		
CTOS Modem Service Operations and Programming Guide Literature Set	5.1	4393 0502-000
Which includes:		
CTOS Modem Service Operations and Programming Guide	5.1	
3/4-inch binder and slipcase		
To order individual items:		
CTOS Remote Access Facility (RAF) Software Release Announcement (SRA)	R3.2.0	4393 3217-001
CTOS Remote Access Facility (RAF) Installation, Administration, and Operations Guide	R3.2	4393 5931-000
CTOS Remote Access Facility (RAF) Action Key Quick Reference	R3.2	4393 5949-000
CTOS Modem Service Operations and Programming Guide	5.1	3912 6107-000

43933217-001